OBJETIVO ESTRATÉGICO ENCS-2030	OBJETIVO ESPECÍFICO	LINEA DE ACCIÓN	ACTIVIDAD	2022	2023	2024
		1.1.1 Fortalecer las entidades y organismos bri	1.1.1.1 Fortalecimiento Instituciones que brindan atención y respuesta a incidentes cibernéticos			
	1.1	recursos tecnológicos, financieros, humanos, entre otros.	1.1.1.2 Desarrollar Programa de Capacitación especializada en ciberdelitos a actores del poder judicial			
lal	Fortalecimiento integral de las entidades y organismos	1.1.2 Fortalecer la gobernanza de las entidades y organismos especializados de apoyo, de las instituciones de gestión y de seguimiento a delitos de ciberseguridad	•			
OBJETIVO E. NO. 1 Fortalecimiento Institucional	especializados de apoyo en el ámbito de la	apoyo en el ámbito de la gestión y sensibilización para funcionarios y servidores en materia de ciberseguridad. 1.1.3: Desarrollar planes de formación, capacitación y sensibilización para funcionarios y servidores en materia de ciberseguridad.	1.1.3.1 Implementar Programa de Desarrollo de Competencias en Ciberseguridad			
OBJETIVO E. NO. 1 lecimiento Instituc	seguimiento de ciberseguridad.		1.1.3.2 Incorporar Programas de Concientización para servidores públicos			
OB Fortalec			1.1.4.1 Implementar canales de atención para la recepción de reportes y denuncias vía medios digitales			
		también simplificar dichos trámites	1.1.4.2 Implementar canales presenciales para el reporte de denuncias			
	1.2 Fortalecimiento de las instituciones del Estado en materia de ciberseguridad a	1.2.1 Articular la revisión de las estructuras actuales de tecnologías de la información (TI) de las instituciones del Estado para establecer una estructura independiente, enfocada en la ciberseguridad, conforme a las buenas prácticas internacionales, con fines de priorizar los pilares fundamentales de la seguridad de la información en las instituciones del Estado.	Seguridad de la Información para someter su			

	nivel de estructuras, formación, estándares y lineamientos para el fortalecimiento de la seguridad	1.2.2 Diseñar un plan de formación, capacitación y sensibilización en ciberseguridad para personal responsable de la seguridad de la información en las instituciones del Estado.	1.2.2.1 Elaborar Plan de Capacitación Especializada para personal de seguridad de la información del Estado 1.2.2.2 Elaborar Programa de Sensibilización para responsables de seguridad de la información del Estado			
	de la información.	1.2.3 Elaborar, definir y garantizar cumplimiento de los	1.2.3.1 Elaboración de normas de adquisiciones para el sector público y privado basados en las buenas prácticas internacionales; evaluación de riesgo en inversión.			
		estándares para la seguridad de las Tecnologías de la Información y Comunicación (TIC) en el Estado.	1.2.3.2 Elaboración y Publicación de Estándar de Desarrollo Seguro			
			1.2.3.3 Propuesta de inclusión de norma de adquisición de equipos bienes y servicios tecnológicos para infraestructuras críticas del Estado.			
OBJETIVO E. NO. 2 Protección & Reslisiencia de Infraestructuras Críticas	2.1 Fortalecer la	2.1.1 Elaborar y establecer un plan nacional de respuesta a incidentes de ciberseguridad, y contingencias a riesgos, que procure la adecuada actuación en la gestión de incidentes cibernéticos, riesgos de emergencia y crisis nacional.	2.1.1.1 Elaborar y poner en marcha el Plan Nacional de Respuesta a Crisis Cibernéticas.			
VO E. NO. encia de Ir ríticas	protección de las infraestructuras críticas nacionales y las de tecnologías de la información (TI) del Estado.	2.1.2 Identificar y apoyar los organismos principales en el área de respuesta a incidentes que puedan proporcionar soporte a las infraestructuras críticas nacionales y las e tecnologías de la información (TI) del Estado y del sector privado en función al Plan Nacional de Respuesta a Incidentes de de descripción de la información (TI) del Estado y del sector privado en función al Plan Nacional de Respuesta a Incidentes de	organizaciones de apoyo para la la respuesta			
OBJETIVO E. ón & Reslisiencia Crítica			2.1.2.2 Revisar y establecer los mecanismos de cooperación			
Protecció		2.1.3 Desarrollar y establecer los protocolos de activación y acción para los organismos de respuesta, y todo el ciclo de gestión de los incidentes.	2.1.3.1 Desarrollo del protocolo de activación y acción para la gestión de incidentes cibernéticos			

		2.1.4 Elaborar y establecer un plan nacional de comunicación e intercambio de información ante crisis de incidentes de seguridad cibernética.				
		2.1.5 Fortalecer los Equipos Sectoriales de Respuestas a Incidentes Cibernéticos (CSIRT) y promover el	2.1.5.1 Extender Formaciones Especializadas para los Equipos de Respuestas a Incidentes Sectoriales			
		establecimiento de estos en los sectores críticos nacionales.	2.1.5.2 Promover el desarrollo de Reglamentos de Ciberseguridad en los Sectores Críticos Nacionales			
		2.1.6 Diseñar, establecer y poner en marcha un plan de ejercicios de simulación de incidentes cibernéticos para las infraestructuras críticas nacionales y las instituciones del Estado.	simulación a nivel nacional y sectorial,			
		2.1.7: Fomentar la concientización y sensibilización en materia de criptografía a nivel del Estado.	2.1.7.1 Desarrollar campaña de concientización focalizada con el enfoque de la criptografía			
		2.2.1 Establecer una metodología común para la gestión de los riesgos cibernéticos, y sus lineamientos, así como los mecanismos de gobernabilidad, para la supervisión,	2.2.1.1 Desarrollar Plataforma y definir Metodología del Marco Gobernanza			
	2.2 Fortalecer la gestión de riesgos, identificar las infraestructuras críticas nacionales y las infraestructuras	evaluación y medición periódica de implementación y cumplimiento de las políticas de tecnologías de información, los planes de riesgos y de continuidad operativa, en conformidad con las mejores prácticas, y alineada a los estándares y metodologías internacionales para las infraestructuras criticas nacionales y de las instituciones del Estado, y promover su adopción en el sector privado.	2.2.1.2 Desarrollar Evaluaciones de Madurez Instituciones del Estado			
	de tecnologías de la información (TI) relevantes del Estado y efectuar un análisis de riesgo.	2.2.2 Establecer los criterios que determinan el grado de criticidad de una infraestructura, basado en los estándares internacionales en la materia.	2.2.2.1 Elaborar y Socializar Criterios IIC			
		2.2.3 Catalogar las infraestructuras críticas nacionales e infraestructuras tecnologías de la información (TI) relevantes del Estado de acuerdo con los criterios que determinan su grado de criticidad, incluyendo los servicios colaterales que las soportan.	2.2.3.1 Elaboración del Catálogo de Sectores			

		2.2.4 Efectuar análisis de riesgo sobre las infraestructuras críticas nacionales e infraestructuras tecnologías de la información (TI) relevantes del Estado y determinar su nivel de vulnerabilidad, contemplando la inclusión de los perfiles de riesgos sectoriales más críticos para la sociedad y la economía nacional.				
	2.3 Elaborar los reglamentos, normas, estándares y lineamientos	2.3.1 Evaluar las normas y reglamentaciones emitidas por reguladores sectoriales para someter propuestas de actualizaciones a estos órganos, atendiendo a estándares internacionales.	2.3.1.1 Identificación y Revisión de los Reglamentos Existentes y Normas emitidas en materia de Ciberseguridad			
	para el fortalecimiento de la	2.3.2 Apoyar la elaboración y el establecimiento de reglamentos sectoriales y en el diseño del modelo de	2.3.2.1 Coordinación y Apoyo para el desarrollo Reglamentos Sector Eléctrico			
	coordinación y respuesta a incidentes de ciberseguridad en	gobernanza del sector.	2.3.2.2 Coordinación y Apoyo para el desarrollo Reglamentos Sector Transporte Marítimo			
	las infraestructuras críticas nacionales y de tecnologías de la información (TI) del Estado.	2.3.3 Elaborar y establecer los protocolos de intercambio de información entre los Equipos Sectoriales de Respuestas a Incidentes Cibernéticos (CSIRT), las instituciones del Estado, las infraestructuras críticas y el Equipo Nacional de Respuesta a Incidentes Cibernéticos (CSIRT-RD), para la gestión de los incidentes de ciberseguridad	2.3.3.1 Desarrollar y socializar Protocolos de Intercambios			
E. NO. 3 & Cultura	3.1. Fomentar la inclusión de la formación y sensibilización en	3.1.1 Establecer una política de desarrollo de competencias digitales en la población con énfasis en la ciberseguridad, contemplando programas de educación, formación técnica, sensibilización y concientización para lograr un ciberespacio más seguro.	3.1.1.1 Diseñar política de desarrollo de competencias digitales en ciberseguridad para la población			
OBJETIVO E. NO. 3 Educación & Cultura	ciberseguridad en todos los niveles del sistema educativo.	3.1.2 Fortalecer los programas de educación en ciberseguridad de las instituciones de educación superior y técnicos, en los diferentes niveles de grado, técnico, licenciatura, maestrías y doctorado, para aumentar la disponibilidad y calidad de las ofertas académicas y profesionales especializados.	3.1.2.1 Realizar levantamiento de las ofertas académicas de Ciberseguridad brindadas por las IES e institutos técnicos superiores			

	3.1.2.1 Elaborar propuestas de actualización para fortalecer los programas académicos ofertados en materia de ciberseguridad			
3.1.3 Incorporar contenidos básicos de ciberseguridad, en las asignaturas de tecnología de información de los programas de formación de las diferentes carreras, en	3.1.3.1 Realizar levantamiento de los programas de las asignaturas TIC ofertadas en los pensum de las IES e institutos Técnicos superiores de las diferentes carreras			
las instituciones de educación y técnicos superiores para fortalecer la concienciación y cultura de la ciberseguridad a nivel profesional.	3.1.3.2 Elaborar propuesta de actualización de contenidos de ciberseguridad para el pénsum de las asignaturas ofertadas en las diferentes carreras por las IES e Institutos Técnicos Superiores			
3.1.4 Incorporar en el programa de educación básica e intermedia, contenidos de ciberseguridad para fortalecer la sensibilización, concienciación y cultura de la ciberseguridad en los estudiantes y profesores de esos niveles.	3.1.4.1 Elaborar propuesta de contenido para la inclusión de contenidos de ciberseguridad en las escuelas públicas y colegios privados			
3.1.5 Diseñar un programa de cooperación para la implementación de formaciones especializadas en coordinación con las instituciones académicas.	=			
3.1.6 Implementar sistema de certificación emitida por institución acreditada para formación especializada en ciberseguridad.	3.1.6.1 Diseñar y poner en marcha certificación de acreditación para formación en Ciberseguridad			
3.1.7 Diseñar e implementar programas de pasantías para fomentar nuevos talentos en materia de ciberseguridad con el apoyo y cooperación de las instituciones de educación intermedia, superior y técnicos profesional.	Pasantías en el Centro Nacional de			

		3.1.8 Diseñar un programa de desarrollo de cibertalentos para apoyar la demanda de recursos especializados en el sector de la seguridad de la información.	<u> </u>			
		3.1.9 Establecer programas de formación de certificación criptográfica.	3.1.9.1 Diseñar y desarrollar programa especializado de criptografía			
	3.2 Impulsar una cultura nacional	3.2.1 Desarrollar un programa general de concientización para sensibilizar y fortalecer el entendimiento de ciberseguridad, conocer los riesgos, amenazas y forma de abordarlos estos temas, para niños, adolescentes, adultos mayores, MIPYMES, el sector público y privado, entre otros.	_			
	de ciberseguridad en todo el país enfocada a las diferentes poblaciones vulnerables	3.2.2 Desarrollar campañas de sensibilización, en medios tradicionales y digitales, con el apoyo del sector público, privado, la academia, organizaciones de medios y las organizaciones de la sociedad civil para fortalecer la cultura de ciberseguridad, promover la protección en línea de la información personal, y buenas prácticas en el uso de plataformas en línea y redes sociales.	concientización continúas a través de los			
		3.2.3 Implementar programas de reconocimiento para diversos sectores en apoyo a la cooperación en los esfuerzos de concientización y cultura de ciberseguridad a la población.	3.2.3.1 Diseñar Programa de reconocimiento y fomentar participación sectores			
OBJETIVO E. NO. 4 Alianzas Nacionales e Internacionales	4.1 Realizar alianzas nacionales e	4.1.1 Establecer acuerdos marcos de cooperación técnica, operativa y de capacitación para el fortalecimiento de la ciberseguridad.				
OBJETIVO E. NO. Alianzas Nacionale Internacionales	internacionales para fortalecer la cooperación.	4.1.2 Fomentar alianzas con el sector privado, organizaciones de la sociedad civil y la academia para fortalecer la confianza ciudadana en la seguridad cibernética.	4.1.2.1 Elaborar el Plan y establecer acuerdos de cooperación con Sector Privado y la Academia			

		_	4.1.3.1 Identificar Organizaciones Claves Internacionales y Establecer Acuerdo de Cooperación de Ciberseguridad.			
		4.1.4 Asegurar la participación de la República Dominicana en los foros internacionales de	4.1.4.1 Identificación y Levantamiento de Eventos importantes de Ciberseguridad anual			
		ciberseguridad.	4.1.4.2 Coordinar la participación en los eventos internacionales.			
		4.1.5 Monitorear y evaluar el nivel de cumplimiento país con los acuerdos y gobernanza del ciberespacio a nivel internacional	•			
berseguridad		5.1.1 Promover programas de emprendimiento e innovación en la industria de ciberseguridad.	5.1.1.1 Diseñar un programa de apoyo y fomento para los emprendimientos en la industria de ciberseguridad nacional con los sectores público, privado y sociedad civil.			
5 tria de Ci	5 4 5amantan la		5.1.1.2 Puesta en marcha del Plan para el Programa de Emprendimientos			
OBJETIVO E. NO. 5 Desarrollo e Investigación de la Industria de Ciberseguridad	5.1 Fomentar la investigación, el desarrollo y la innovación de la ciberseguridad y su entorno.	5.1.2 Incentivar las investigaciones para el fortalecimiento y desarrollo de capacidades a nivel país.	5.1.2.1 Elaborar el Plan de alianzas con los actores del sistema nacional de educación superior y organismos internacionales para implementar programas avanzados de investigación en ciberseguridad.			
C			5.1.2.2 Diseñar y publicar campañas focalizada para el fomento de las investigaciones en Ciberseguridad			
Desarrollo e		5.1.3 Desarrollar estudios, y promover la generación de estadísticas y creación de indicadores para apoyar en el desarrollo de políticas públicas, basadas en evidencias, vinculado al ecosistema de ciberseguridad	·			

		5.1.4 Realizar encuestas regionales o nacionales, análisis de datos, y evaluaciones para medir el impacto de la Estrategia Nacional de Ciberseguridad 2030 en diferentes sectores.	sobre Ciberseguridad para evaluar la				
		5.1.5 Promover estudios de investigación en el desarrollo y adopción de nuevas tecnologías disruptivas y su impacto en la ciberseguridad.	5.1.5.1 Desarrollar Estudio sobre Riesgo e Impacto Nuevas Tecnologías Disruptivas				
			6.1.1.1 Actualización de la Estrategia Nacional de Ciberseguridad 2030				
0		6.1.1Monitorear, revisar y analizar el marco legal y normativo vinculado a la ciberseguridad, ciberdefensa, ciberguerra, ciberterrorismo y ciberdelito, y proponer	CITIZE TRANSPORTER TO PROSTE TRANSPORTER				
6 o Jurídico	6.1Fortalecer y garantizar el cumplimiento de	6.1Fortalecer y garantizar el un plan de actualización que garanticen un ecosistema nacional seguro, frente al contexto de nuevas amenazas y riesgos cibernéticos producto de las tecnologías emergentes, velando por la protección de los derechos humanos en línea, la niñez y el consumidor en línea, la protección de datos personales, las prioridades nacionales y los estándares internacionales relevantes.	6.1.1.3 Elaboración Propuesta Anteproyecto Ley Gestión de Ciberseguridad				
OBJETIVO E. NO. 6 imiento del Marco	las normativas legales, técnicas y regulatorias de ciberseguridad al		6.1.1.4 Elaboración Propuesta Actualización Ley No. 53-07 - Sobre Crímenes y Delitos de Alta Tecnología				
OBJE1 rtalecimien	contexto actual		6.1.1.5 Realizar evaluaciones bianuales del marco legal y regulatorio de la República Dominicana				
Fo		6.1.2 Elaborar las normativas y los estándares técnicos aplicables a la ciberseguridad y promover su adopción.	6.1.2.1 Elaboración Política de Divulgación Vulnerabilidades				
		6.1.3: Impulsar el cumplimiento de las normativas en materia de ciberseguridad por parte de los organismos de la administración pública.	6.1.3.1 Elaboración Decreto - Notificación Obligatoria				