REAL

RED DE EXPERTOS Y ANALISTAS LATINOAMERICANOS

CEXCCR

PLAN ESTRATÉGICO 2024 - 2028

INNOVACIÓN. COOPERACIÓN. RESILIENCIA

REAL

RED DE EXPERTOS Y ANALISTAS LATINOAMERICANOS

CENTRO DE EXCELENCIA DE COOPERACION CIBERNETICA REGIONAL

PLAN ESTRATÉGICO 2024 - 2028

Pioneros en un futuro cibernético innovador, cooperativo y resiliente para América Latina

Documento elaborado por la Red de Expertos y Analistas Latinoamericanos

CONTENIDO

PRÓLOGO

RESUMEN EJECUTIVO

INTRODUCCIÓN

- Desafíos y oportunidades para América Latina
- Nuestra visión: Innovación, cooperación y resiliencia
- Los pilares de nuestra estrategia
- Meta y objetivos

PARTE 1: ESTRATEGIA

CONTEXTO ESTRATÉGICO

- Objetivos
- Actividades
- Indicadores de Impacto

PARTE 2: IMPLEMENTACIÓN

TRABAJANDO POR NUESTRA AMBICIÓN

- Marco Internacional
- Indicadores de Éxito
- Plan de Gestión de la Calidad.
- Plan de Gestión de Riesgos.
- Identificación y Evaluación Cualitativa de Riesgos.
- Plan de Respuesta a Riesgos.
- Plan de Participación de Interesados

PARTE 3: CONCLUSIONES

CONCLUSIONES

APÉNDICES

PRÓLOGO
RED DE EXPERTOS Y ANALISTAS LATINOAMERICANOS

La Red de Expertos y Analistas Latinoamericanos (REAL) se presenta como una organización no gubernamental internacional (ONGI) independiente, registrada en Washington, D.C., y reconocida por el IRS como exenta de impuestos según la Sección 501(c)(3) del Código de Rentas Internas. Nuestra misión es promover la seguridad, la defensa, el desarrollo y la democracia en América Latina mediante servicios de asesoría, consultoría y ejecución de proyectos.

En REAL, creemos en el poder del esfuerzo colectivo y las iniciativas conjuntas para lograr cambios significativos. Nuestra fortaleza radica en el conocimiento y la experiencia de un equipo diverso de profesionales multidisciplinarios, cuidadosamente seleccionados, con una trayectoria comprobada en quince países de América y Europa. Nuestros expertos son egresados de prestigiosas instituciones, incluyendo el Centro William J. Perry de Estudios Hemisféricos de Defensa y la Universidad de Defensa Nacional, compartiendo valores y principios con estas renombradas entidades.

A pesar de nuestra corta historia, nos hemos consolidado rápidamente como un socio confiable, capaz de ejecutar proyectos con éxito y evitar errores de improvisación. Nuestra metodología de trabajo única y no tradicional nos permite abordar desafíos complejos mientras mantenemos un enfoque cohesivo, coordinando actividades, compartiendo conocimientos y aprendiendo mutuamente. Esta sincronización potencia el impacto de nuestro trabajo, permitiéndonos ofrecer soluciones innovadoras adaptadas a cada contexto.

REAL está comprometida a ser un catalizador de transformación positiva, abordando preocupaciones globales como el cambio climático, la resolución de conflictos y la protección de los derechos humanos. A través de alianzas estratégicas, enfoques basados en la investigación e intervenciones prácticas, aspiramos a contribuir a un mundo donde la paz, la estabilidad y el progreso sean accesibles para todos.

GONZALO RAMOS LEMA
Presidente

SOBRE REAL
RED DE EXPERTOS Y ANALISTAS LATINOAMERICANOS

MISIÓN

Brindar servicios de consultoría y asesoría estratégica profesionales, innovadores y personalizados a organizaciones, instituciones y gobiernos en Seguridad, Defensa, Desarrollo y Democracia en la región.

SERVICIOS

CONSULTORÍA
REAL ofrece servicios de consultoría y asesoría en democracia, desarrollo, defensa y seguridad con integridad y calidad. Soluciones innovadoras y personalizadas para gobiernos y organizaciones.

INVESTIGACIÓN Y CONOCIMIENTO
R.E.A.L. investiga y gestiona conocimiento en áreas críticas (seguridad, salud, educación, etc.), brindando soluciones prácticas y rentables para transformar sociedades.

GESTIÓN DE PROYECTOS
REAL ofrece soluciones innovadoras y adaptadas a problemas sociales cruciales en democracia, gobernanza, derechos humanos y desarrollo protege a poblaciones vulnerables.

ANÁLISIS POLÍTICO
REAL es una ONG dedicada al análisis multidisciplinario regional para la seguridad hemisférica y la integridad. Nuestros expertos informan y promueven soluciones inclusivas.

RESUMEN EJECUTIVO

CENTRO DE EXCELENCIA DE COOPERACION CIBERNETICA REGIONAL

En el rápido y evolutivo panorama de la ciberseguridad y el desarrollo digital, América Latina se encuentra en una encrucijada crucial caracterizada por una mezcla de amenazas, vulnerabilidades y oportunidades. La Estrategia de Ciberseguridad para América Latina en 2023 subraya la importancia de la colaboración, la innovación y la responsabilidad como pilares clave para navegar por este entorno complejo. Este momento tiene el potencial de que la región invierta estratégicamente en sus capacidades cibernéticas, aprovechando tanto los sectores públicos como privados para una defensa efectiva contra las amenazas emergentes.

América Latina enfrenta una mezcla dinámica de desafíos en ciberseguridad, que van desde amenazas cibernéticas en evolución dirigidas a infraestructuras críticas y filtraciones de datos, hasta el aumento de redes delictivas cibernéticas que explotan vulnerabilidades digitales. Simultáneamente, la proliferación de tecnologías digitales y la convergencia de información crean un terreno fértil tanto para el crecimiento económico como para un aumento de los riesgos cibernéticos. La trayectoria futura de la región radica en integrar los esfuerzos en ciberseguridad y seguridad digital para fomentar un ecosistema digital seguro. Esta convergencia demanda acciones coordinadas entre sectores y fronteras para mejorar la resiliencia cibernética en general. Reconocer a la Red de Expertos y Analistas Latinoamericanos, una organización internacional con una amplia presencia en 12 países latinoamericanos y una experiencia diversa, abre vías para esfuerzos colaborativos que abarcan sectores y fronteras.

Colaborar con la REAL presenta una oportunidad única para catalizar las capacidades cibernéticas en toda la región. Aprovechar a sus expertos multidisciplinarios equipados con destrezas técnicas ofrece un enfoque integral para abordar los desafíos de ciberseguridad. Esta asociación podría facilitar un escenario de cooperación triangular, fomentando soluciones interdisciplinarias para el complejo panorama cibernético de la región.

INTRODUCCIÓN

DESAFIOS Y OPORTUNIDADES PARA AMÉRICA LATINA

En el mundo actual, marcado por la creciente interconexión digital, la ciberseguridad emerge como un pilar fundamental para proteger la integridad, privacidad y continuidad de organizaciones y naciones. La rápida evolución tecnológica y la expansión del ciberespacio han proporcionado innumerables beneficios, pero también han dado lugar a una compleja red de amenazas cibernéticas que pueden tener un impacto devastador en nuestra sociedad, economía y seguridad nacional. La ciberseguridad no solo se trata de proteger sistemas y redes, sino también de preservar la confianza en la tecnología que impulsa nuestra vida diaria. En este contexto, el fortalecimiento de las defensas cibernéticas, la promoción de la conciencia en seguridad digital y la cooperación entre sectores y naciones se vuelven esenciales para garantizar un entorno cibernético seguro y resiliente en el que podamos aprovechar plenamente los beneficios de la era digital.

La región de América Latina se encuentra inmersa en una notable transformación impulsada por avances tecnológicos exponenciales y costos decrecientes, lo que ha dado lugar a una conectividad sin precedentes. Adicionalmente, la pandemia de COVID-19 ha acelerado aún más esta tendencia, impulsando un cambio estructural profundo y duradero, que trae consigo amplias oportunidades, innovación y crecimiento. Sin embargo, esta transformación digital, mayor conectividad, y acceso de internet ha expuesto a América Latina a amenazas cibernéticas más intensas debido a una superficie de ataque ampliada. A pesar de un progreso significativo, la región aún lidia con disparidades en las medidas de ciberseguridad, la falta de legislación y normas, la escasez de talento y alianzas y asociaciones regionales limitadas.

Asimismo, la falta histórica de conciencia en ciberseguridad entre individuos, empresas y entidades gubernamentales en América Latina los hace particularmente vulnerables a amenazas como la ingeniería social, el phishing y el cibercrimen. Esta problemática se agrava debido a la asignación insuficiente de recursos para la ciberseguridad en la región, lo que obstaculiza el desarrollo de defensas sólidas, la capacitación de profesionales y la adopción de tecnologías avanzadas de detección de amenazas. Los sectores críticos de infraestructura, como energía, transporte y salud, exhiben debilidades que, si se explotaran, podrían causar trastornos económicos y sociales significativos. Por otro lado, debido a la inestabilidad política, la región también se ve inmersa en ataques con motivación política respaldados por el estado que han previamente afectado a instituciones gubernamentales, medios de comunicación y organizaciones civiles, e inclusive elecciones, profundizando la inestabilidad e ingobernabilidad en diferentes países de la región.

INTRODUCCIÓN

DESAFIOS Y OPORTUNIDADES PARA AMÉRICA LATINA

La interconexión global expone a las empresas y gobiernos latinoamericanas a riesgos cibernéticos a través de terceros. En la actualidad, los países latinoamericanos desarrollan sus estrategias de seguridad en el ciberespacio de forma aislada o contando con pocas iniciativas de integración y trabajo mancomunado. Para abordar estos problemas y fomentar la cooperación regional, la Red de Expertos y Analistas Latinoamericanos ha desarrollado una estrategia regional basada en un enfoque integral de soluciones adaptables y de capacitación para promover la cooperación y el liderazgo en el ciberespacio aprovechando directrices y marcos internacionales. Mientras países latinoamericanos buscan definir sus roles en un entorno competitivo en constante evolución, fortalecer su poder cibernético se convierte en un imperativo estratégico. El fortalecimiento de las capacidades cibernéticas no solo les permitirá liderar el avance en la industria, sino que también les posibilitará anticipar cambios tecnológicos futuros, mitigar amenazas y ganar ventaja sobre sus competidores.

El plan estratégico del Centro de Excelencia en Cooperación Cibernética Regional (CexCCR) tiene como misión actuar como un catalizador para potenciar las capacidades en el ámbito ciberespacial tanto en el sector público como en el privado. Mediante la creación de entornos de colaboración y trabajo interdisciplinario, buscamos abordar los desafíos que el ciberespacio plantea a la región. Nuestra iniciativa promueve la cooperación entre naciones y organizaciones privadas, ofreciendo un enfoque distintivo en cuestiones críticas de defensa y seguridad cibernética. El CexCCR se presenta como un integrador de estrategias de ciberseguridad en la región, a través del amplio conocimiento y la experiencia especializada por parte de un grupo de expertos internacionales, que mediante investigaciones, programas de capacitación y ejercicios prácticos, buscamos proporcionar soluciones integrales y avanzadas.

América Latina tiene la oportunidad de aprovechar estos desafíos de una manera integral y colaborativa, empoderando a individuos y organizaciones a liderar en el ciberespacio con responsabilidad y eficacia para asegurar intereses colectivos, promover la inclusividad y ejercer influencia en el panorama cibernético global. La propuesta de la Red de Expertos y Analistas Latinoamericanos con el Centro de Excelencia en Cooperación Cibernética Regional (CexCCR) juegan un papel crítico al unir fuerzas, compartir conocimientos y avanzar hacia una ciberseguridad más robusta y resiliente en la región.

VISIÓN

INNOVACIÓN, COOPERACIÓN Y RESILIENCIA

Nuestra visión para el Plan Estratégico CExCCR es forjar canales de cooperación del sector público y privado de naciones afines, ofreciendo un enfoque interdisciplinario único a los temas más relevantes de la defensa y seguridad cibernética con nuestra investigación, capacitaciones especializadas y ejercicios prácticos, que abarquen todas las dimensiones de la seguridad digital. Nuestro plan se sustenta en tres pilares fundamentales que hemos identificado como esenciales para alcanzar nuestra visión:

1

INNOVACIÓN

Reconocemos que el panorama cibernético está en constante evolución, con amenazas y desafíos que cambian rápidamente. Por lo tanto, nuestra estrategia se centra en fomentar la innovación continua en el ámbito de la ciberseguridad. A través de la investigación y el desarrollo de nuevas soluciones, nos esforzamos por anticipar y abordar las amenazas emergentes, y así, promovemos la adopción de tecnologías y enfoques avanzados que fortalezcan la defensa cibernética.

COOPERACIÓN

2

Reconocemos que la ciberseguridad es un desafío global que requiere un enfoque colaborativo. Nuestro plan se enfoca en facilitar y fomentar la cooperación entre el sector público y privado de naciones afines. A través de alianzas estratégicas, intercambio de conocimientos y mejores prácticas. Buscamos crear un ecosistema de colaboración que permita compartir información relevante y responder de manera conjunta a las amenazas cibernéticas.

3

RESILIENCIA

Reconocemos que la resiliencia cibernética es fundamental para garantizar la continuidad de las operaciones y la seguridad en un entorno digital. Nuestra estrategia se centra en fortalecer la resiliencia de las organizaciones y gobiernos mediante la capacitación, la planificación de incidentes y la implementación de estrategias de mitigación de riesgos. Aspiramos a que las naciones afines estén mejor preparadas para enfrentar y recuperarse de los ataques cibernéticos.

En conjunto, estos pilares definen una hoja de ruta para que el CExCCR se convierta en un líder en el ámbito cibernético, con el firme compromiso de empoderar a las naciones afines a enfrentar los desafíos cibernéticos actuales y futuros, esperamos contribuir significativamente a un ciberespacio más seguro y robusto en toda la región.

OFERTA DE VALOR

1

Contamos con profesionales multidisciplinarios con experiencia extensa y probada en campo en catorce países de los continentes americano y europeo. Cada miembro es un pilar esencial en la organización tiene el conocimiento y la experiencia técnica necesaria para abordar temas relevantes, lo que nos permite ser un socio bien posicionado y confiable con la capacidad de llevar a cabo cualquier proyecto con éxito evitando errores derivados de la improvisación.

2

Trabajamos en cada país de residencia, coordinando actividades, compartiendo conocimientos y aprendiendo el uno del otro para que nuestro trabajo sea sincronizado. Ofrecemos soluciones donde organizaciones vinculadas a EEUU no tienen la llegada o injerencia suficiente para generar un cambio estructural de alto impacto. Nos responsabilizamos de todos los proyectos y resultados sin vincular necesariamente a organizaciones de cooperación o financiamiento.

3

La ventaja de establecer una organización en Estados Unidos radica en la robusta estructura legal y reguladora, lo que brinda mayor seguridad y confianza tanto a la organización como a las agencias federales al garantizar el cumplimiento de estándares de transparencia y protección de datos. Sin embargo, nuestro trabajo coordinado trasciende fronteras nacionales, lo que nos permite generar un impacto positivo a nivel regional como una extensión de los intereses compartidos con EEUU.

PARTE 1

METAS Y OBJETIVOS

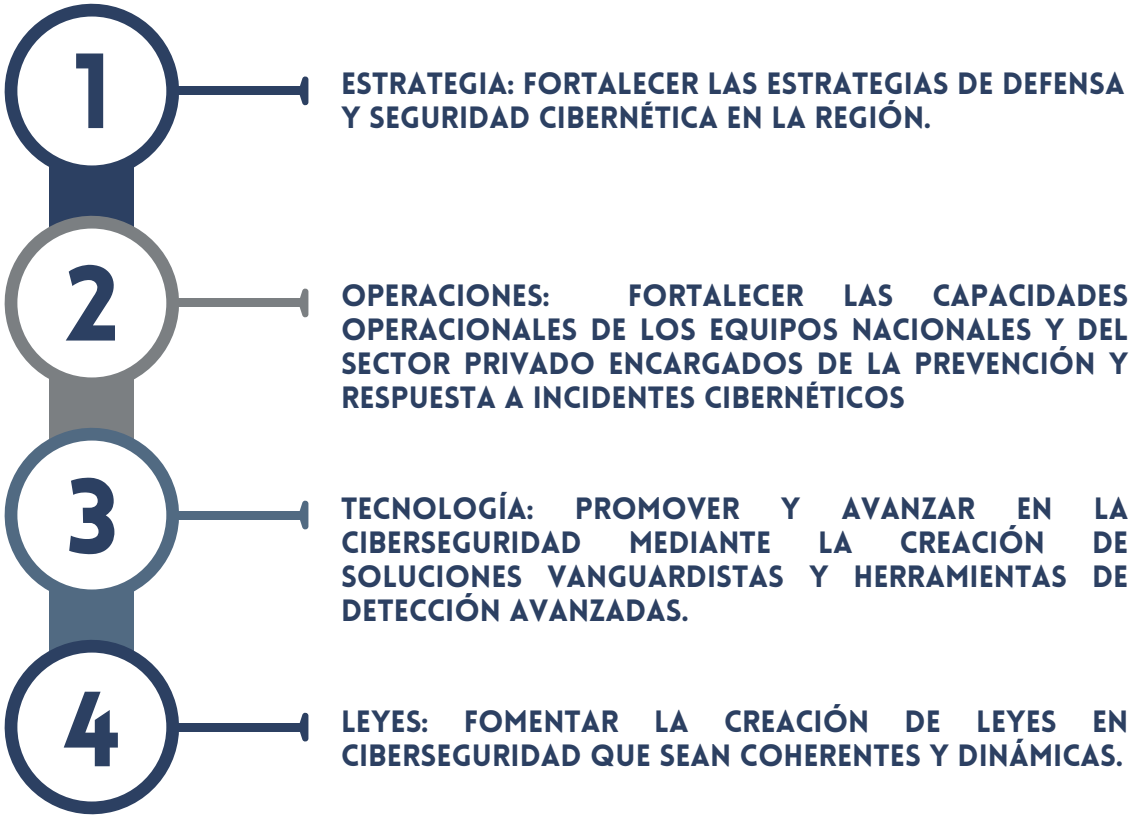
METAS Y OBJETIVOS

MISIÓN

El Plan Estratégico del Centro de Excelencia en Cooperación Cibernética Regional (CexCCR) tiene como misión actuar como un catalizador para potenciar las capacidades en el ámbito ciberespacial tanto en el sector público como en el privado.

En el marco de nuestra estrategia integral de ciberseguridad, delineada en el Plan Estratégico CexCCR, se han establecido metas y objetivos conexas que guiarán nuestras acciones. Estas metas se traducirán en acciones concretas a través de la implementación de Planes Operativos Anuales y la ejecución de proyectos específicos que serán sometidos a una evaluación rigurosa. Es crucial resaltar que los objetivos fundamentales que hemos establecido no operan de manera independiente, sino que están interconectados y se complementan mutuamente. Nuestra estrategia se erige sobre la premisa de que la fortaleza en un área fortalece y respalda el logro de los demás objetivos, en una sinergia que optimiza nuestra capacidad para salvaguardar la seguridad cibernética en su conjunto.

OBJETIVOS



ESTRATEGIA

OBJETIVO 1

En vista de la creciente relevancia de la ciberseguridad en un mundo digital interconectado, el CexCCR se enfoca en una prioridad crucial: mejorar las estrategias de protección cibernética en organizaciones y naciones afines. Nuestro centro se dedicará a brindar servicios especializados de asesoramiento, capacitación y apoyo a líderes de alto nivel, con el fin de fomentar un enfoque proactivo y coordinado en la formulación de estrategias de ciberseguridad en diferentes entornos.

Objetivo 1.1 Cooperación triangular: Nuestro enfoque se centra en establecer y fortalecer asociaciones estratégicas con diversas instituciones a nivel regional, incluyendo entidades gubernamentales, instituciones académicas y empresas del sector privado. Esta colaboración en tres direcciones posibilita un intercambio valioso de conocimientos, las prácticas más efectivas y sinergia al abordar de amenazas cibernéticas que trascienden fronteras geográficas.

Objetivo 1.2 Asesoramiento Estratégico: Proporcionaremos orientación de carácter teórico con un enfoque prospectivo para la ciberseguridad, anticipando tendencias y desarrollos en el ciberespacio. Ofreceremos asesoramiento concreto en la aplicación de estrategias y medidas de ciberseguridad. De esta forma, aseguramos que las ideas adquiridas se conviertan en acciones reales y efectivas. Esto engloba la evaluación de los riesgos cibernéticos, la formulación de recomendaciones políticas y estratégicas, así como la elaboración de planes de respuesta en caso de incidentes.

Objetivo 1.3 Cadena de conocimiento: Nuestra iniciativa se enfoca en establecer colaboraciones sólidas con un sector clave, instituciones académicas. Esta colaboración estratégica será la base para el ciclo de conocimiento, mejorando la efectividad de profesionales en todos los rangos de ciberseguridad, y la toma de decisiones respaldada. A través del centro, se llevarán a cabo conferencias, seminarios y eventos de acceso público que servirán como plataformas para compartir conocimientos y fomentar diálogos en torno a los temas de seguridad digital. Además, nuestro equipo generará informes y publicaciones especializadas con el fin de mantener a la comunidad informada sobre las últimas tendencias y desafíos en constante evolución en este dominio de conocimiento.

ESTRATEGIA

OBJETIVO 1

IMPACTO ESPERADO

El establecimiento del CexCCR contribuirá al fortalecimiento de la seguridad cibernética a nivel regional al facilitar la colaboración internacional, elevar los estándares de ciberseguridad en organizaciones y gobiernos, y promover la innovación en la lucha contra las amenazas cibernéticas.

INDICADORES DE IMPACTO

Nuestro proyecto se orienta hacia la consecución de resultados concretos y medibles. Estableceremos tres indicadores clave que reflejarán el éxito y la eficacia de nuestras actividades en el ámbito de la ciberseguridad.

1 | Participación de Líderes y Tomadores de Decisiones en la Red de Cooperación Regional: Mediremos nuestro impacto a través del número de líderes y miembros de alto nivel, incluyendo personal C-level, que se involucran activamente en nuestra red de colaboración regional. Esta métrica demostrará nuestra capacidad para reunir a las partes interesadas más influyentes y comprometidas en la esfera de la ciberseguridad, promoviendo así la cooperación efectiva y el intercambio de conocimientos.

2 | Aplicación de Conocimientos y Lecciones Aprendidas en la Formulación de Estrategias y la Toma de Decisiones: Evaluaremos el éxito de nuestro enfoque al medir la utilización de los conocimientos adquiridos y las lecciones aprendidas en el proceso de diseño de estrategias y la toma de decisiones. Si nuestras actividades contribuyen directamente a la formulación de estrategias más informadas y a decisiones más acertadas en materia de ciberseguridad, habremos logrado un impacto sustancial en la resiliencia cibernética de las organizaciones y naciones implicadas.

3 | Impacto de la Red de Cooperación e Intercambio en Entornos Menos Maduros en Ciberseguridad: Centramos nuestra atención en evaluar el impacto de nuestra red de cooperación y el intercambio de conocimientos en organizaciones y naciones que aún están desarrollando su madurez en ciberseguridad. Medimos cómo estas entidades adoptan y adaptan las mejores prácticas y estrategias compartidas, fortaleciendo sus propias posturas en ciberseguridad. Este indicador resalta nuestra capacidad para influir positivamente en contextos donde la ciberseguridad se encuentra en una etapa incipiente, demostrando la amplitud de nuestro impacto.

Estos indicadores cuantitativos nos proporcionarán una visión objetiva y verificable del progreso de nuestro proyecto y su efecto en la seguridad cibernética. Estamos comprometidos con la generación de resultados tangibles y positivos que respalden la mejora continua en la gestión de amenazas cibernéticas a nivel regional y global.

OPERACIONES

OBJETIVO 2

El segundo objetivo que abordamos se centra en reforzar las habilidades operativas de los equipos nacionales y del sector privado responsables de prevenir y responder ante incidentes cibernéticos, tales como los CERT (Equipo de Respuesta a Emergencias Informáticas), CSIRT (Equipo de Respuesta a Incidentes de Seguridad Informática) y SOC (Centro de Operaciones de Seguridad).

Objetivo 2.1 Ejercicios Especializados: Desarrollaremos programas de formación y ejercicios específicos adaptados a las necesidades y niveles de experiencia de los participantes. Estos programas abarcarán ejercicios que simulan ataques, situaciones de incidentes del mundo real y prácticas de respuesta coordinada. A través de estas actividades, buscamos fortalecer las habilidades de los equipos para lidiar con situaciones reales de manera efectiva y colaborativa.

Objetivo 2.2 Red de asesoramiento multidisciplinario: Estableceremos una red de expertos activos y disponibles en toda la región, formada para abordar de manera integral los aspectos técnicos, legales y de políticas en ciberseguridad. Este enfoque multidisciplinario nos permitirá reunir a profesionales en ciberseguridad, ingenieros, analistas forenses, expertos legales y otros especialistas pertinentes. Así, podremos abordar los desafíos cibernéticos desde diversas perspectivas, garantizando respuestas más sólidas y completas.

Objetivo 2.3 Capacidad de resiliencia cibernética: Nuestro enfoque se centra en reducir los incidentes en infraestructuras críticas y redes gubernamentales, así como en disminuir el tiempo que los actores maliciosos permanecen en los sistemas. Esto implica el desarrollo y la promoción de estrategias que mejoren la capacidad de recuperación de sistemas y redes cibernéticos. Nuestro objetivo es minimizar tanto el impacto como la duración de los ataques cibernéticos, fortaleciendo así la seguridad y estabilidad de las entidades.

OPERACIONES

OBJETIVO 2

IMPACTO ESPERADO

El CexCCR empoderará a los equipos y a las organizaciones para que puedan responder con rapidez y eficacia a los desafíos en constante evolución en el panorama de la ciberseguridad, contribuyendo significativamente a la respuesta coordinada frente a las amenazas cibernéticas en constante evolución.

INDICADORES DE IMPACTO

Nuestra evaluación se basará en indicadores sólidos que reflejen el efecto real y positivo de nuestras iniciativas en el ámbito de la ciberseguridad. Estos indicadores son diseñados para medir los resultados tangibles y cuantificables de nuestro trabajo.

1 | Fortalecimiento de Capacidades: Mediremos el éxito de; CexCCR a través del aumento en la capacidad de las organizaciones para identificar, prevenir y responder a amenazas cibernéticas de manera eficaz y coordinada. Observaremos mejoras en las operaciones de los equipos CSIRT, CERT, y SOC, tanto a nivel nacional como privado. Este progreso se evidenciará mediante la aplicación de formación especializada y ejercicios prácticos diseñados para potenciar sus habilidades operativas.

2 | Colaboración Transfronteriza en Ciberseguridad: Mediremos el impacto de las iniciativas de cooperación regional destinadas a fortalecer la lucha contra las amenazas cibernéticas que traspasan fronteras. Esta medición se realizará tanto en términos cuantitativos como cualitativos, evaluando las medidas adoptadas para fomentar la confianza en la digitalización y las operaciones en línea a nivel regional. Nuestro objetivo es incrementar la confianza y la colaboración entre naciones, permitiendo una respuesta más sólida y coordinada ante las amenazas cibernéticas transfronterizas.

3 | Reducción de Incidentes y Persistencia de Actores Adversos: Uno de nuestros criterios fundamentales de éxito radicará en la disminución de la cantidad de incidentes que afectan a infraestructuras críticas y redes gubernamentales, así como en la reducción del impacto de dichos incidentes. Asimismo, evaluaremos la disminución del tiempo que los actores adversos permanecen en cada incidente. Estos indicadores nos proporcionarán una visión clara de nuestra contribución a la mitigación de amenazas cibernéticas y al fortalecimiento de la capacidad de recuperación de organizaciones y naciones ante ataques cibernéticos.

TECNOLOGÍA

OBJETIVO 3

*Nuestro objetivo es promover y avanzar en la ciberseguridad mediante la creación de soluciones vanguardistas y herramientas de detección avanzadas. Para lograrlo, estableceremos un ecosistema integral que conecte investigación, desarrollo y colaboración entre la comunidad académica y la industria. Este enfoque estimulará la innovación y permitirá que las soluciones más avanzadas lleguen al mercado, garantizando una mayor protección en el paisaje digital actual.

Objetivo 3.1 Programas de Incubación y Aceleración: Implementaremos programas de incubación y aceleración dirigidos a startups y proyectos emprendedores centrados en la ciberseguridad. Estos programas proporcionarán recursos, orientación y apoyo para convertir ideas innovadoras en soluciones concretas. Al proporcionar un entorno de desarrollo favorable, impulsaremos la creación de tecnologías disruptivas y su rápida introducción en el mercado.

Objetivo 3.2 Colaboración entre la Comunidad Académica y la Industria: Facilitaremos la colaboración entre investigadores académicos y profesionales de la industria cibernética. Organizaremos eventos, talleres y conferencias que fomenten el intercambio de conocimientos y la cooperación en la búsqueda de soluciones de ciberseguridad avanzadas. Esta sinergia permitirá que las investigaciones de vanguardia sean aplicadas en entornos prácticos y beneficiosos.

Objetivo 3.3 Adopción de Tecnologías Emergentes:

- Plataforma en la Nube: Aprovecharemos los beneficios de la tecnología en la nube para acelerar el desarrollo y la implementación de soluciones de seguridad. La agilidad y escalabilidad de las plataformas en la nube permitirán la rápida iteración y adaptación de las soluciones a las demandas cambiantes del entorno cibernético.
- Inteligencia Artificial Adaptativa: Emplearemos técnicas de inteligencia artificial (IA) para crear soluciones adaptativas capaces de detectar patrones de amenazas cambiantes y ajustar sus estrategias de defensa en consecuencia. La IA mejorará la detección temprana y la respuesta a amenazas desconocidas.
- Metaverso: Consideraremos las implicaciones de seguridad en los entornos de metaverso, donde la interconexión digital se vuelve aún más compleja. Desarrollaremos enfoques de seguridad para asegurar la privacidad y la integridad en este espacio emergente.
- Tecnología Sostenible: Nos comprometemos a desarrollar soluciones de ciberseguridad que sean compatibles con prácticas tecnológicas sostenibles. La seguridad cibernética no sólo debe protegernos, sino también contribuir a la preservación del medio ambiente.

TECNOLOGÍA

OBJETIVO 3

IMPACTO ESPERADO

Mediante la convergencia de estos componentes, nuestro objetivo es catalizar el desarrollo de tecnologías de seguridad revolucionarias, reforzando la ciberseguridad en un entorno digital en constante evolución.

INDICADORES DE IMPACTO

1 | Conversión de Ideas a Soluciones Comerciales: Mediremos la efectividad de nuestros programas al evaluar la proporción de ideas innovadoras que se transforman en soluciones concretas listas para el mercado. Esta tasa reflejará la capacidad de nuestros programas para catalizar la innovación y llevar las ideas de seguridad cibernética desde la conceptualización hasta la implementación práctica.

2 | Nivel de Adopción de Investigaciones Académicas: Mediremos el impacto de la colaboración al evaluar cuántas investigaciones académicas relevantes se han aplicado efectivamente en soluciones de seguridad cibernética en el mercado. Esto se reflejará en la cantidad de soluciones que incorporan conceptos y enfoques provenientes de investigaciones académicas, mostrando cómo la sinergia entre la academia y la industria se traduce en avances tangibles.

3 | Velocidad de Desarrollo y Despliegue en la Nube: Mediremos el tiempo que toma desde la concepción hasta la implementación de soluciones de seguridad en la nube. Una reducción en este tiempo indicará la agilidad y eficacia de nuestro enfoque en la nube para el desarrollo y la adaptación de soluciones cibernéticas en respuesta a amenazas cambiantes.

4 | Mejora en la Detección y Respuesta a Amenazas: Cuantificáremos la disminución en el tiempo que lleva detectar, analizar y responder a amenazas cibernéticas gracias a la implementación de soluciones de inteligencia artificial adaptativa. Esto demostrará cómo nuestra estrategia de IA mejora la eficacia y eficiencia de la ciberdefensa.

5 | Nivel de Seguridad en Entornos de Metaverso: Evaluar la adopción y eficacia de las soluciones de seguridad en el contexto del metaverso, midiendo la capacidad de estas soluciones para salvaguardar la privacidad y la integridad en un espacio digital cada vez más complejo.

LEYES

OBJETIVO 4

El siguiente objetivo que hemos establecido se alinea estrechamente con las prioridades que hemos identificado en los antecedentes de nuestra estrategia, y aborda uno de los desafíos más significativos que afectan a la ciberseguridad en nuestra región. Este desafío en particular se relaciona con la falta de regulaciones y normativas sólidas en el ámbito de la ciberseguridad. Nuestro enfoque se centrará en fomentar la creación de leyes en ciberseguridad que sean coherentes tanto con las dinámicas locales como con las tendencias globales. Al abordar las deficiencias actuales en la regulación cibernética, estaremos estableciendo los cimientos para fortalecer la defensa y seguridad en este ámbito crítico.

Objetivo 4.1 Análisis de Escenarios: Nuestro enfoque implica llevar a cabo un análisis profundo de los entornos cibernéticos, tanto a nivel local como regional. Esto nos permitirá identificar amenazas emergentes, vulnerabilidades y tendencias en el ámbito de la ciberseguridad. Al anticipar y comprender de manera exhaustiva los riesgos, nuestros expertos en ciberseguridad podrán proponer soluciones adecuadas y efectivas para contrarrestar estas amenazas.

Objetivo 4.2 Desarrollo de Legislación Armonizada: Uno de nuestros objetivos centrales es promover la creación de legislación en ciberseguridad que sea coherente y armonizada a nivel internacional. Trabajaremos en estrecha colaboración con gobiernos y organizaciones relevantes para identificar áreas clave que requieran regulación y, posteriormente, para desarrollar estándares y directrices que sean aplicables en diversas jurisdicciones. Este esfuerzo busca establecer un marco normativo robusto que aborde los desafíos actuales y futuros en ciberseguridad de manera cohesiva.

Objetivo 4.3 Enfoque en Derechos Humanos y Tecnología: Además de nuestro trabajo en la esfera de la ciberseguridad, también abordaremos la intersección entre tecnología y derechos humanos. Creemos firmemente en el potencial de la tecnología para impulsar el desarrollo humano y mejorar la calidad de vida, especialmente en el contexto de avances tecnológicos como la tecnología 4G y futuras innovaciones. Nuestro centro realizará investigaciones exhaustivas y desarrollará recomendaciones para garantizar que el progreso tecnológico vaya de la mano con la protección de los derechos humanos. Esta perspectiva integral nos permitirá aprovechar el poder de la tecnología de manera ética y beneficiosa.

LEYES

OBJETIVO 4

IMPACTO ESPERADO:

Nuestro enfoque integral en legislación en ciberseguridad y tecnología-humanos promete un impacto significativo. Colaborando con expertos globales, fortaleceremos la ciberseguridad mediante conocimiento compartido y respuesta coordinada ante amenazas. Armonizaremos regulaciones para enfrentar desafíos y proteger infraestructuras vitales. Promoveremos tecnología responsable al considerar su impacto en derechos humanos y desarrollo. Al difundir conocimiento, reduciremos brechas en la comprensión cibernética, impulsando conciencia y decisiones informadas. Este compromiso resultará en un entorno digital más seguro y confiable. Con enfoque en colaboración, investigación y ética, trabajamos para fortalecer la ciberseguridad global y mejorar la calidad de vida.

INDICADORES DE IMPACTO:

1 | Preparación ante Amenazas: Se evalúa cómo el desarrollo de leyes y regulaciones sólidas en ciberseguridad, que son coherentes con las dinámicas locales y las tendencias globales, contribuye a mejorar la preparación de la región ante amenazas cibernéticas. Los componentes clave de este indicador incluyen la calidad del marco legal, la capacidad de cumplimiento de las regulaciones, la conciencia pública y la educación en ciberseguridad, la reducción de amenazas cibernéticas específicas y la colaboración internacional en materia de regulación cibernética. Este indicador busca medir el impacto positivo de un entorno legal y normativo sólido en la reducción de riesgos cibernéticos y en la promoción de la seguridad digital en la región.

2 | Índice de Armonización Legal: Se evaluará la efectividad en la promoción de legislación cibernética armonizada. Se considerará la cantidad de acuerdos y colaboraciones internacionales alcanzados para la adopción de estándares y directrices comunes. El porcentaje de jurisdicciones que implementan regulaciones coherentes con los estándares acordados será un indicador de éxito. Una mayor adopción indicará un mayor nivel de armonización normativa y un impacto positivo en la capacidad de responder a amenazas cibernéticas a nivel global.

3 | Índice de Tecnología Responsable: Se evaluará la alineación entre avances tecnológicos y derechos humanos. El índice medirá cómo las innovaciones tecnológicas contribuyen al desarrollo humano y a la calidad de vida, considerando indicadores como la accesibilidad, la privacidad y la igualdad. La proporción de recomendaciones implementadas para asegurar que el progreso tecnológico no infrinja los derechos humanos será un indicador clave. Un aumento en la implementación indicará un mayor impacto en la adopción ética y beneficiosa de tecnologías avanzadas.

PARTE 2

IMPLEMENTACIÓN

MARCO INTERNACIONAL

El CexCCR se alinea perfectamente con marcos y acuerdos internacionales, incluyendo los Objetivos de Desarrollo Sostenible (ODS) de las Naciones Unidas 9, 10, 11, 12 y 17, el Manual de Tallin y el Acuerdo de la Organización de Cooperación de Shanghái (SCO). Al incorporar estos marcos en nuestra estrategia, buscamos fomentar la colaboración, la inclusión, el desarrollo sostenible y una mayor resiliencia en ciberseguridad en la región.

ALINEACIÓN CON LOS OBJETIVOS DE DESARROLLO SOSTENIBLE (ODS) DE LA ONU

- **ODS 9: Industria, Innovación e Infraestructura:** El plan estratégico enfatiza el desarrollo y la mejora de la infraestructura de ciberseguridad e innovación en la región. Al fomentar avances tecnológicos y promover un ecosistema de ciberseguridad robusto, contribuimos a los objetivos del ODS 9 de construir infraestructuras resilientes y promover una industrialización inclusiva y sostenible.
- **ODS 10: Reducción de las Desigualdades:** Para abordar la brecha digital y reducir las desigualdades, nuestro plan enfatiza la capacitación y el intercambio de conocimientos. Al garantizar que todas las naciones dentro de la región tengan acceso a recursos y experiencia en ciberseguridad, buscamos reducir las disparidades en capacidades de ciberseguridad en alienación con los objetivos del ODS 10.
- **ODS 11: Ciudades y Comunidades Sostenibles:** Al fomentar ciudades y comunidades ciber-resilientes, nos alineamos con el objetivo del ODS 11 de hacer que las ciudades sean inclusivas, seguras, resilientes y sostenibles.
- **ODS 12: Producción y Consumo Responsables:** Nuestra estrategia promueve el consumo y la producción responsables de bienes y servicios digitales, fomentando prácticas sostenibles y seguras en el ciberespacio. Al promover la conciencia sobre la ciberseguridad y comportamientos responsables, contribuimos al objetivo del ODS 12 de garantizar patrones de consumo y producción sostenibles.
- **ODS 17: Alianzas para lograr los Objetivos:** La colaboración y las alianzas son fundamentales en nuestro plan estratégico. Al promover la colaboración internacional, público-privada y entre sectores, nos alineamos con los objetivos del ODS 17 de fortalecer los medios de implementación y revitalizar la asociación global para el desarrollo sostenible.

Promovemos la cooperación internacional y la adopción de normas para garantizar la seguridad y la paz en el ciberespacio a través de estos marcos establecidos por Naciones Unidas. Estos lineamientos respaldan nuestra búsqueda de un ciberespacio más seguro y confiable en la región americana.

MARCO INTERNACIONAL

ORGANIZACIÓN MUNDIAL DEL COMERCIO (WTO), ORGANIZACIÓN MUNDIAL DE ADUANAS (WCO) Y ORGANIZACIÓN MUNDIAL DE LA PROPIEDAD INTELECTUAL (WIPO)

Nuestra estrategia promueve la colaboración entre organizaciones internacionales clave, incluyendo la WTO, WCO, y WIPO, para abordar cuestiones relacionadas con la ciberseguridad en el contexto del comercio, aduanas y propiedad intelectual. Al asegurar la protección de datos y la ciberseguridad en estas áreas, contribuimos a un entorno digital más seguro y confiable.

ACUERDO DE LA ORGANIZACIÓN DE COOPERACIÓN DE SHANGHÁI (SCO)

El Acuerdo de la SCO se centra en mejorar la cooperación en el campo de las tecnologías de la información y comunicación, incluida la ciberseguridad. El CexCCR se alinea con el Acuerdo de la SCO al enfatizar la colaboración regional y la asistencia mutua para responder de manera efectiva a las amenazas de ciberseguridad. Apoyamos el intercambio de información y los esfuerzos conjuntos para mejorar la seguridad del ciberespacio en la región.

ACUERDO DE BUDAPEST

Nuestra estrategia también se alinea con el Acuerdo de Budapest, que busca promover la cooperación internacional en la lucha contra el cibercrimen. A través de la colaboración y el intercambio de información en ciberseguridad, trabajamos para fortalecer la resiliencia cibernética en la región americana y más allá.

MANUAL DE TALLIN

El Manual de Tallin proporciona orientación sobre el derecho internacional en lo que respecta a las operaciones cibernéticas. EL CexCCR se alinea con los principios del Manual de Tallin al enfatizar el cumplimiento del derecho internacional, normas y comportamiento responsable en el ciberespacio. Abogamos por reglas de compromiso claras y cooperación internacional para mejorar la ciberseguridad y minimizar los riesgos de conflicto cibernético.

GESTIÓN DE ALCANCE

PROCESO DE DEFINICIÓN DE ALCANCE: Descripción detallada del proceso para elaborar el scope statement definitivo a parti del scope statement preliminar. Definición de qué, quién, cómo, cuándo, dónde y con qué.

La definición del Alcance del CexCCR se desarrollará de la siguiente manera:

- En reunión de equipo de proyecto, tanto el equipo de proyecto como el sponsor revisarán el Scope Statement preliminar, el cual servirá como base.

PROCESO PARA ELABORACIÓN DE W BS: Descripción detallada para crear, aprobar y mantener el W BS. Definición de qué, quién, cómo, cuándo, dónde y con qué.

Los pasos que se realizaron para la elaboración del WBS son los siguientes:

- El EDT del proyecto será estructurado de acuerdo a la herramienta de descomposición, identificándose primeramente los principales entregables, que en el proyecto actúan como fases. En el proyecto se identificó 4 fases.
- Identificado los principales entregables, se procede con la descomposición del entregable en paquetes de trabajo, los cuales nos permiten conocer al mínimo detalle el costo, trabajo y calidad incurrido en la elaboración del entregable.
- La empresa utiliza para la elaboración del WBS la herramienta WBS Chart Pro, pues permite una fácil diagramación y manejo de los entregables del proyecto.

PROCESO PARA ELABORACIÓN DEL DICCIONARIO WBS: Descripción detallada del proceso para crear, aprobar y mantener el diccionario WBS. Definición de qué, quién, cómo, cuándo, dónde y con qué.

Previo a este proceso, el WBS del proyecto debe haber sido elaborado, revisado y aprobado. Es en base a la información del WBS que se elaborará el Diccionario WBS, para lo cual se realizarán los siguientes pasos:

- La elaboración del Diccionario WBS se hace mediante una plantilla diseñada por el CexCCR.
- Se identifica las siguientes características de cada paquete de trabajo del WBS.
- Se detalla el objetivo del paquete de trabajo.
- Se hace una descripción breve del paquete de trabajo.
- Se describe el trabajo a realizar para la elaboración del entregable, como son la lógica o enfoque de elaboración y las actividades para elaborar cada entregable.
- Se establece la asignación de responsabilidad, donde por cada paquete de trabajo se detalla quién hace qué: responsable, participa, apoya, revisa, aprueba y da información del paquete de trabajo.
- De ser posible se establece las posibles fechas de inicio y fin del paquete de trabajo, o un hito importante.
- Se describe cuáles son los criterios de aceptación

GESTIÓN DE ALCANCE

PROCESO PARA VERIFICACIÓN DE ALCANCE: Descripción detallada del proceso para la verificación formal de los entregables y su aceptación por parte del cliente (interno o externo). Definición de qué, quién, cómo, cuándo, dónde y con qué.

Al término de elaboración de cada entregable, éste debe ser presentado al Sponsor del Proyecto, el cual se encargará de aprobar o presentar las observaciones del caso. Si el entregable es aprobado,
es enviado al cliente.

PROCESO PARA CONTROL DE ALCANCE: Descripción detallada del proceso para identificar, registrar y procesar cambios de alcance, asi como su alcance con el control integrado de cambios. Definición de qué, quién, cómo, cuándo, dónde y con qué.

En este caso se presentan dos variaciones:

- **Primero:** el Project Manager se encarga de verificar que el entregable cumpla con lo acordado en la Línea Base del Alcance. Si el entregable es aprobado es enviado al interesado, pero si el entregable no es aprobado, el entregable es devuelto a su responsable junto con una hoja de correcciones, donde se señala cuáles son las correcciones o mejoras que se deben hacer.
- **Segundo:** a pesar que el Project Manager se encarga de verificar la aceptación del entregable del proyecto, el interesado también puede presentar sus observaciones respecto al entregable, para lo cual requerirá reunirse con el Project Manager, y presentar sus requerimientos de cambio o ajuste. De lograrse la aceptación del interesado y de tratarse de un entregable muy importante, se requerirá la firma de un acta de aceptación del entregable.

PLAN DE GESTIÓN
DE CALIDAD

POLÍTICA DE CALIDAD DEL PROYECTO: Especificar la intención de dirección que formalmente tiene el equipo de proyecto con relación a la calidad del programa.
Este proyecto debe cumplir con los requisitos de calidad desde el punto de vista de REAL, es decir acabar dentro del tiempo y el presupuesto planificados, y también debe cumplir con los requisitos de calidad del interesado, es decir prestar el servicio y obtener un buen nivel de satisfacción por parte del interesado.

LÍNEA BASE DE CALIDAD DEL PROYECTO: Factores de calidad relevantes para el producto y gestión del programa. Para cada factor de calidad relevante, definir los objetivos de calidad, las métricas a utilizar y las frecuencias de medición y de reporte.

FACTOR DE CALIDAD RELEVANTE	OBJETIVO DE CALIDAD	MÉTRICA A UTILIZAR	FRECUENCIA Y MOMENTO DE MEDICIÓN	FRECUENCIA Y MOMENTO DE REPORTE
Perfomance del Proyecto	CPI>= 0.95	CPI= Cost Performance Index Acumulado	Frecuencia, semanal. Medición, lunes en la mañana.	Frecuencia semanal Reporte, lunes en la tarde
Perfomance del Proyecto	SPI >= 0.95	SPI= Schedule Performance Index Acumulado	Frecuencia, semanal Medición, lunes en la mañana	Frecuencia semanal Reporte, lunes en la tarde
Satisfacción de los interesados	Nivel de Satisfacción >= 4.0	Nivel de Satisfacción= Promedio entre 1 a 5 de 14 factores sobre Material, personal, y servicio	Frecuencia, una encuesta por cada servicio Medición, al día siguiente de la encuesta	Frecuencia, una vez por cada servicio Reporte, al día siguiente de la medición

PLAN DE MEJORA DE PROCESOS: Pasos para analizar procesos, los cuales facilitaran la identificación de actividades que generan desperdicio o que no agregan valor:

1. Delimitar el proceso
2. Determinar la oportunidad de mejora
3. Tomar información sobre el proceso
4. Analizar la información levantada
5. Definir las acciones correctivas para mejorar el proceso
6. Aplicar las acciones correctivas
7. Verificar si las acciones correctivas han sido efectivas
8. Estandarizar las mejoras logradas para hacerlas parte del proceso

IDENTIFICACIÓN Y EVALUACIÓN CUALITATIVA DE RIESGOS

PROBABILIDAD	VALOR NUMERICO	IMPACTO	VALOR
MUY IMPROBABLE	0.1	Muy Bajo	0.05
RELATIVAMENTE PROBABLE	0.3	Bajo	0.10
PROBABLE	0.5	Moderado	0.20
MUY PROBABLE	0.7	Alto	0.40
CASI CERTEZA	0.9	Muy Alto	0.80

TIPO DE RIESGO	PROBABILIDAD X IMPACTO
Muy Alto	Mayor a 0.50
ALto	Menor a 0.50
Moderado	Menor a 0.30
Bajo	Menor a 0.10
Muy Bajo	Menor a 0.10

1. Ver Anexo 1, tabla de los riesgos identificados.

PARTE 3

CONCLUSIONES

El plan estratégico de la Red de Expertos y Analistas Latinoamericanos (REAL) establece una base sólida para abordar los desafíos y riesgos cibernéticos emergentes en América Latina mediante una visión centrada en la cooperación regional y la integración de esfuerzos.

Este enfoque integral posiciona a REAL como un catalizador en la construcción de resiliencia cibernética, fomentando alianzas estratégicas entre sectores públicos y privados y facilitando un intercambio continuo de conocimientos y mejores prácticas en ciberseguridad.

Al integrar innovación, capacitación y colaboración, REAL no solo refuerza las capacidades técnicas de los actores clave en la región, sino que también promueve un ecosistema de seguridad digital que favorece la estabilidad y el progreso económico en América Latina. La cooperación intersectorial y transfronteriza planteada en este plan es crucial para desarrollar soluciones eficaces y sostenibles, contribuyendo así a un ciberespacio seguro y confiable que responde a las necesidades actuales y futuras de la región.

ANEXO 1

IDENTIFICACIÓN Y EVALUACIÓN CUALITATIVA DE RIESGOS

DESCRIP. DEL RIESGO	CAUSA RAIZ	TRIGGER	ENTREGABLES AFECTADOS	EST. DE PROB.	OBJ. AFECTADO	EST. DE IMPACTO	PROB X IMPACTO	TIPO DE RIESGO
Modificación del cronograma	Solicitud del comite de control de cambios	Conversaciones o Consultas informales	2.0 planeamiento 3.0 Ejecucion	0.3	Tiempo	0.20	0.06	Bajo
Baja satisfacción de los interesados con los servicios prestados	No cumplimiento de los objetivos de calidad	Resultados de encuestas	Programa completo	0.3	-Costo -Calidad	-0.10 -0.50	-0.03 -0.15	Moderado
Meterial insuficiente o con deficiencias de contenido	Falta de material	Resultados de las encuestas	3.0 Ejecución	0.3	-Tiempo -Costo -Calidad	-0.20 -0.20 -0.20	-0.06 -0.06 -0.06	Moderado
Metodología inadecuada para la prestación del servicio	Metodologia de servicio empleada	Resultados de encuestas	3.0 Ejecución 4.0 Seguimiento	0.1	-Calidad	-0.30	-0.03	Muy bajo
Solicitud de adicionales no contemplados en el alcance	Identificación de nuevos entregables	Conversaciones o consultas informales Resultados de las encuestas	Programa completo	0.2	-Tiempo -Costo	-0.10 -0.10	-0.02 -0.02	Muy bajo
Incumplimientos de los contratos	Falta de coordinación y comunicación con los proveedores	Detección de pequeños incumplimientos o signos de no calidad de servicio	3.0 Ejecución 4.0 Seguimiento	0.5	-Costo -Calidad	-0.30 -0.40	-0.15 -0.20	Alto

ANEXO 1

IDENTIFICACIÓN Y EVALUACIÓN CUALITATIVA DE RIESGOS

DESCRIP. DEL RIESGO	CAUSA RAIZ	TRIGGER	ENTREGABLES AFECTADOS	EST. DE PROB.	OBJ. AFECTADO	EST. DE IMPACTO	PROB X IMPACTO	TIPO DE RIESGO
Desaprobación de los informes mensuales o informe anual	El informe no esta de acuerdo a los terminos de referencia del contrato	Conversaciones o Consultas informales	5.0 Informes	0.3	Tiempo -Costo	-0.10 -0.10	-0.03 -0.03	Bajo
Incumplimiento de los contratos de provisión de insumos	Deficiencias en el servicio del proveedor	Detección de pequeños incumplimientos o signos de no calidad de servicio	3.0 Ejecución 4.0 Seguimiento	0.3	-Costo -Calidad	-0.30 -0.50	-0.09 -0.15	Moderado

REAL

RED DE EXPERTOS Y ANALISTAS LATINOAMERICANOS

CONTÁCTENOS

@ingoreal

@red_real_latam

Red de Expertos y Analistas Latinoamericanos

+ 1 202 826-9000

info@real-oneamerica.org

3097 Desmond Place Ijamsville, MD – 21754 USA