GOBIERNO DE ARAGON

Estrategia en materia de Ciberseguridad Comunidad Autónoma de Aragón

MAYO 2024

ÍNDICE

1 Misión y valores de la estrategia

MISIÓN Y VALORES DE LA ESTRATEGIA

Definición de la misión que guía la estrategia de ciberseguridad

En un entorno global donde los riesgos de ciberseguridad están en constante evolución, el Gobierno de Aragón reconoce la importancia de proteger los recursos y servicios digitales gubernamentales para garantizar la seguridad y privacidad de la información de los ciudadanos.

Actualmente, las amenazas no sólo son más avanzadas, sino que también afectan una mayor superficie de ataque, desde infraestructuras críticas hasta dispositivos personales y sistemas en la nube. Nos encontramos en una era digital que presenta desafíos únicos y oportunidades significativas.

A través de la innovación, la educación y la implementación de las mejores prácticas en seguridad de la información, se promueve el fortalecimiento de la confianza en los servicios digitales del Gobierno de Aragón. Existe también un compromiso para identificar las amenazas de ciberseguridad emergentes y adaptarse continuamente para proteger la infraestructura digital y los datos confidenciales de los ciudadanos.

La misión del Gobierno de Aragón de salvaguardar los servicios digitales ofrecidos a los ciudadanos lleva a establecer un entorno digital seguro y confiable que proteja la integridad, confidencialidad y disponibilidad de los datos sensibles y la información personal de los ciudadanos.

El enfoque está centrado en la prevención proactiva, la detección temprana y la respuesta eficiente a las amenazas cibernéticas, trabajando en colaboración con agencias gubernamentales, empresas privadas y expertos en ciberseguridad para anticipar y mitigar los riesgos de seguridad, garantizando la continuidad de los servicios críticos para el bienestar y la comodidad de los ciudadanos.

MISIÓN Y VALORES DE LA ESTRATEGIA

Definición de la misión que guía la estrategia de ciberseguridad

El Gobierno de Aragón está profundamente comprometido con la implementación de una **estrategia de ciberseguridad robusta y dinámica** que refleje la importancia de:

Conciencia institucional

Ser conscientes de que los riesgos cibernéticos son una amenaza constante a la integridad y privacidad de la información del ciudadano.

Inversión en seguridad

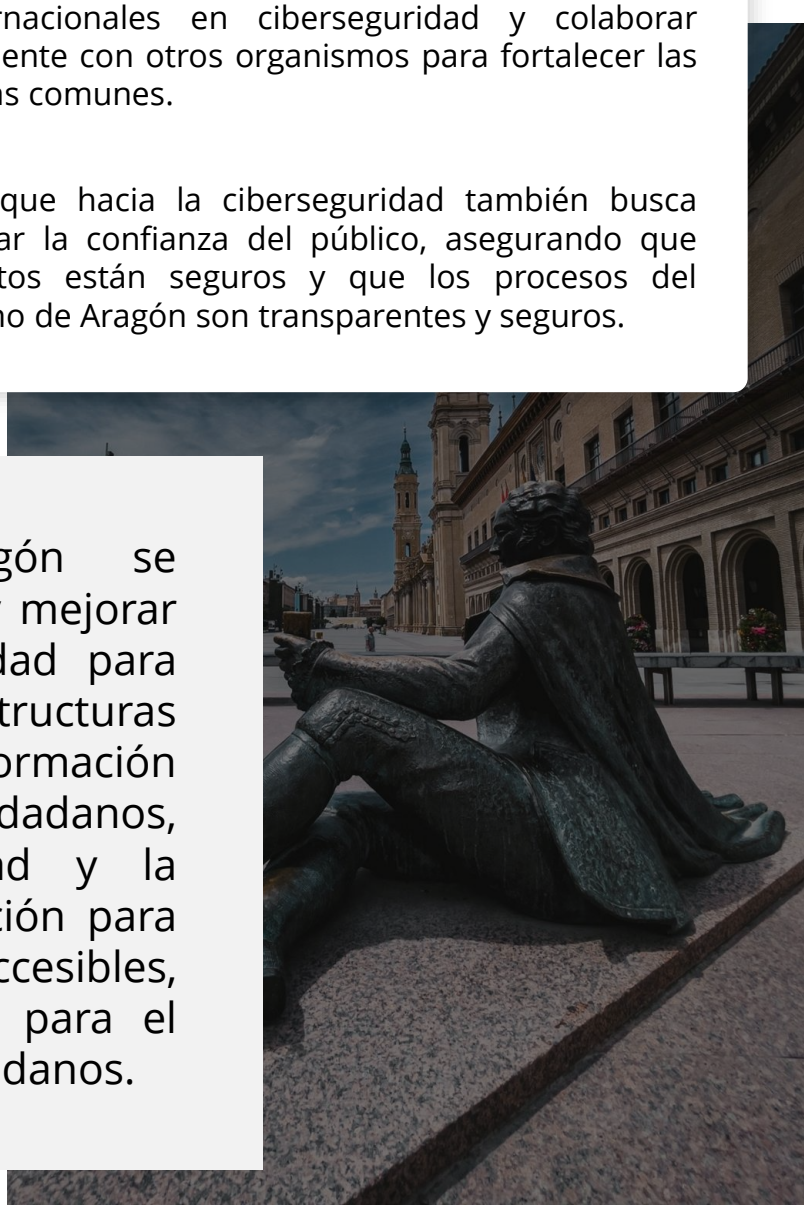
Estar comprometidos en invertir en soluciones de seguridad avanzadas y en la capacitación continua del personal para enfrentar estos desafíos.

Cumplimiento y colaboración

Cumplir rigurosamente con las normativas nacionales e internacionales en ciberseguridad y colaborar activamente con otros organismos para fortalecer las defensas comunes.

Transparencia y confianza

El enfoque hacia la ciberseguridad también busca fomentar la confianza del público, asegurando que sus datos están seguros y que los procesos del Gobierno de Aragón son transparentes y seguros.



El Gobierno de Aragón se compromete a mantener y mejorar continuamente su capacidad para proteger sus infraestructuras tecnológicas y la información personal de los ciudadanos, garantizando la seguridad y la confianza en cada interacción para ofrecer servicios accesibles, eficientes y transparentes para el beneficio de todos los ciudadanos.

MISIÓN Y VALORES DE LA ESTRATEGIA

Valores fundamentales que orientan las decisiones y acciones en materia de ciberseguridad

Confidencialidad:	Asegurar que el acceso a los activos TIC se limite a usuarios y entidades debidamente autorizados, cumpliendo con todas las normas de secreto y sigilo profesional.
Integridad y Calidad:	Mantener la exactitud y corrección de la información y sus procesos asociados mediante mecanismos robustos que aseguren la calidad y veracidad de los datos.
Disponibilidad y continuidad:	Garantizar un alto nivel de disponibilidad de los activos TIC y desarrollar planes de continuidad para responder eficazmente ante contingencias graves.
Trazabilidad:	Implementar medidas que permitan identificar claramente quién realizó qué acción y cuándo, facilitando el análisis detallado de los incidentes de seguridad.
Autenticidad:	Verificar y confirmar la fuente de los datos para garantizar que la información proviene de entidades confiables.
Gestión del Riesgo y Seguridad Integral:	Conducir un proceso continuo de análisis y gestión de riesgos que sirva como base para la seguridad de los activos TIC.
Proporcionalidad en Coste:	Equilibrar los costes al implementar medidas de mitigación de riesgos, asegurando eficiencia y efectividad.
Concienciación y Formación:	Desarrollar programas de educación sobre seguridad TIC para todos los usuarios, enfocándose en derechos y deberes relacionados con la gestión segura de la información.
Prevención, Detección, Respuesta y Conservación:	Crear una estrategia de seguridad que integre prevención, detección y respuesta a incidentes para minimizar vulnerabilidades y reducir el impacto de las amenazas.
Vigilancia, Mejora Continua y Reevaluación Periódica:	Revisar y mejorar los controles de seguridad para adaptarlos a la evolución constante de los riesgos y la tecnología.
Seguridad en el Ciclo de Vida de los Activos TIC:	Incorporar especificaciones de seguridad en todas las fases del ciclo de vida de los sistemas y servicios, asegurando controles efectivos en cada etapa.
Defensa en Profundidad:	Adoptar un enfoque de múltiples capas de seguridad que proteja la información incluso si una capa es comprometida, minimizando el impacto global.
Función Diferenciada:	Diferenciar claramente las responsabilidades de seguridad de las de gestión del servicio e información, asegurando roles y responsabilidades específicos y bien definidos.
Seguridad Global:	Mantener la seguridad por defecto en todas las decisiones y configuraciones, aislando cualquier sistema que reduzca el nivel de seguridad para evitar riesgos adicionales.

El objetivo de los principios de seguridad TIC es establecer un entorno tecnológico seguro, eficiente y confiable. Estos valores no solo dictan cómo usar tecnologías y procedimientos seguros, sino que también fomentan una cultura de seguridad que permea todas las actividades del organismo.

2 Contexto de la ciberseguridad

ENTORNO GLOBAL DE LA CIBERSEGURIDAD

Según datos recientes, se ha observado un aumento en el número de incidentes de ciberseguridad. INCIBE gestionó más de 118,000 incidentes durante 2022, lo que representa un incremento del 9% en comparación con 2021.

El sector de la administración pública registró el 19% de los incidentes, siendo uno de los más afectados, seguido por sectores como el de la salud, banca, transporte y energía. Específicamente, el sector salud es crítico debido a la alta valoración de los datos personales que maneja, lo que lo convierte en un objetivo principal para ataques de ciberdelincuentes que buscan lucrarse a través del robo de información sensible.

El phishing sigue siendo uno de los métodos de ataque más comunes, destacando también la importancia de las vulnerabilidades en sistemas tecnológicos que pueden poner en riesgo la seguridad de las organizaciones. Además, la adopción del trabajo remoto ha incrementado la necesidad de proteger las conexiones inalámbricas y dispositivos utilizados fuera de las oficinas tradicionales.

Para enfrentar estos desafíos, se han desarrollado varias iniciativas y programas. Por ejemplo, el Plan Estratégico Plurianual de INCIBE para 2023-2025 establece directrices y estrategias para mejorar la resiliencia de las infraestructuras críticas frente a los ciberataques. Además, se promueve la colaboración público-privada como un modelo efectivo para fortalecer las capacidades de ciberseguridad a nivel nacional.

El establecimiento de un plan de contingencia y la continua formación en ciberseguridad son esenciales para preparar a las organizaciones para responder efectivamente a los incidentes. Esto incluye desde la protección de la información hasta la implementación de buenas prácticas en la gestión de la identidad online y la autenticación.

CONTEXTO DE LA CIBERSEGURIDAD

Estrategia de ciberseguridad de la UE para la Década Digital

AUMENTO DE EXPOSICIÓN A CIBERAMENAZAS	La transformación digital es una prioridad estratégica para la Unión Europea, pero esta transformación también conlleva un incremento en la exposición a las ciberamenazas. Con el aumento de dispositivos conectados, las redes que conforman la Internet de las Cosas (IoT) elevan las oportunidades y la exposición para los ataques ciber.
IMPACTO DE LA COVID-19 EN LA CIBERSEGURIDAD	La pandemia ha exacerbado las vulnerabilidades cibernéticas, particularmente en sectores críticos como el de la salud. El teletrabajo y el distanciamiento físico han intensificado la dependencia de la tecnología, aumentando así el riesgo de ciberataques y ciberdelincuencia.
INCREMENTO DE CIBERATAQUES, AMENAZAS HÍBRIDAS Y DESINFORMACIÓN	Los ciberataques están aumentando de forma significativa entre las instituciones públicas y privadas, combinándose con campañas de desinformación para influir en los procesos democráticos y económicos en Europa. Estos ataques híbridos representan un problema creciente tanto en el espacio cibernético como en el físico.
FRAGMENTACIÓN DEL MERCADO Y DEPENDENCIA TECNOLÓGICA:	Existe una preocupación sobre la fragmentación del mercado único debido a las normativas nacionales divergentes en materia de ciberseguridad y la dependencia de tecnologías extranjeras, lo que puede afectar la autonomía estratégica de la Unión Europea.
DESAFÍOS EN LA COLABORACIÓN Y LA CIBERINTELIGENCIA	La colaboración en ciberinteligencia y la respuesta colectiva a los ciberataques son áreas en las que aún no se ha alcanzado un acuerdo completo a nivel de la Unión Europea. Esto resalta la necesidad de una estrategia más cohesiva y coordinada.
DESARROLLO DE NORMATIVAS Y ESTRATEGIAS DE CIBERSEGURIDAD	La UE está promoviendo el desarrollo de una legislación horizontal que abarque los requisitos de ciberseguridad para productos y servicios conectados a internet, buscando evitar la fragmentación del mercado y reforzar la seguridad desde el diseño.
RESPUESTAS ESTRATÉGICAS A LAS CIBERAMENAZAS	La UE está enfocada en integrar la ciberseguridad en todas sus políticas digitales y estrategias de financiación, reconociendo que la digitalización implica todos los sectores y que las deficiencias en uno pueden afectar a otros.

CONTEXTO DE LA CIBERSEGURIDAD

Estrategia Nacional de Ciberseguridad 2019

La Estrategia Nacional de Ciberseguridad de 2019 se presenta como una respuesta integral y actualizada a los desafíos emergentes en el ciberespacio, con el objetivo de proteger los activos nacionales y fortalecer la resiliencia contra las ciberamenazas. Los principales puntos incluyen:

Cooperación Público-Privada:
Se enfatiza la importancia de la colaboración entre el gobierno, la industria, y la academia para desarrollar una defensa cibernética robusta.

Educación y Concienciación:
Incrementar la concienciación sobre ciberseguridad entre los ciudadanos y empresas para fortalecer la postura general de seguridad.

Refuerzo de Infraestructuras Críticas:
Asegurar y mejorar la resiliencia de las infraestructuras esenciales para mantener la funcionalidad nacional en situaciones de crisis.

La Estrategia Nacional de Ciberseguridad de 2019 refleja unos retos y perspectivas futuras a tener en cuenta en el ámbito de la ciberseguridad. Dichos retos son:

Desarrollo de Capacidades:
La estrategia reconoce la necesidad de desarrollar capacidades técnicas y humanas en ciberseguridad, incluyendo la formación de expertos y la investigación avanzada en la materia.

Adaptación a Nuevas Tecnologías:
A medida que emergen nuevas tecnologías como la inteligencia artificial y el Internet de las Cosas, la estrategia se adapta para enfrentar los retos que estas tecnologías presentan en términos de seguridad.

CONTEXTO DE LA CIBERSEGURIDAD

Estrategia de Seguridad Nacional 2021

La Estrategia de Seguridad Nacional 2021 refleja un enfoque holístico y proactivo hacia la ciberseguridad, reconociendo su papel central en la defensa de la seguridad nacional en un mundo digitalizado y conectado. Esta estrategia no solo aborda las amenazas actuales, sino que también prepara a España para los desafíos futuros en el ámbito de la ciberseguridad.

DESARROLLO DE CAPACIDADES Y COOPERACIÓN

Capacidades Nacionales:
La Estrategia subraya la importancia de desarrollar capacidades nacionales robustas en ciberseguridad, incluyendo tanto la tecnología como los recursos humanos capacitados.

Cooperación Internacional:
Se enfatiza la cooperación con organismos internacionales y países aliados para fortalecer la defensa colectiva contra las ciber amenazas, con un enfoque que va más allá de las fronteras nacionales.

INNOVACIÓN TECNOLÓGICA

Adopción Tecnológica:
La Estrategia reconoce los retos y oportunidades que presenta la rápida adopción de tecnologías avanzadas, como la inteligencia artificial y la computación cuántica, para la seguridad nacional.

Seguridad de infraestructuras críticas:
Se destaca la necesidad de proteger infraestructuras críticas, que son cada vez más dependientes de sistemas cibernéticos avanzados.

CAMBIOS EN EL ENTORNO DE AMENAZAS

Evolución de Amenazas:
El documento identifica una creciente sofisticación y frecuencia de los ciberataques, lo que requiere una respuesta más dinámica y adaptativa.

Amenazas Híbridas:
Se hace especial mención a las amenazas híbridas, que combinan elementos cibernéticos con tácticas de desinformación y de influencia, complicando la detección y respuesta.

ESTRATEGIAS Y MEDIDAS PROPUESTAS

Planificación Estratégica:
La Estrategia propone un enfoque integrado que abarca desde la prevención y detección hasta la respuesta y recuperación ante ciberincidentes.

Educación y Concienciación:
Se propone mejorar la educación y concienciación en ciberseguridad entre la población general y los sectores clave para fortalecer la postura general de seguridad.

CONTEXTO DE LA CIBERSEGURIDAD

Identificación de desafíos específicos

El panorama de ciberseguridad se ve dominado por ataques cada vez más sigilosos y rápidos, donde los ciberdelincuentes utilizan técnicas sofisticadas como el uso de credenciales legítimas y herramientas para permanecer indetectables. Además, la adopción global de la nube ha hecho incrementar la superficie de exposición de las organizaciones, por lo que son mayores los desafíos en la protección de datos y sistemas.

La expansión de la superficie de exposición en el Gobierno de Aragón implica un mayor número de vectores de ataque posibles, incluyendo dispositivos móviles, sistemas en la nube, y el incremento de conexiones remotas. Este entorno ampliado requiere una vigilancia y una gestión de riesgos constantes para proteger la información crítica y los servicios públicos de posibles compromisos.

CUMPLIMIENTO NORMATIVO

El Gobierno de Aragón enfrenta un panorama regulatorio cada vez más complejo, con normativas nacionales e internacionales que exigen un cumplimiento riguroso. La no adherencia a estas normativas puede resultar en sanciones severas, pérdida de reputación, y otros impactos negativos. Identificar y mitigar los riesgos normativos es clave para garantizar la continuidad y legalidad de las operaciones.

Incumplimiento de Normativas de Protección de Datos:
El Gobierno de Aragón enfrenta un panorama regulatorio cada vez más complejo, con normativas nacionales e internacionales que exigen un cumplimiento riguroso. La no adherencia a estas normativas puede resultar en sanciones severas, pérdida de reputación, y otros impactos negativos. Identificar y mitigar los riesgos normativos es clave para garantizar la continuidad y legalidad de las operaciones.

DESAFÍOS:

Cambios Regulatorios:
La introducción de nuevas leyes o la modificación de las vigentes pueden crear desafíos de cumplimiento inesperados.

Interpretación de Normativas:
Diferencias en la interpretación de normativas pueden resultar en incumplimientos no intencionados.

Exposición Internacional: Las operaciones en múltiples jurisdicciones aumentan la complejidad del cumplimiento debido a la diversidad de requisitos legales.

MANTENER LA INTEGRIDAD

La integridad en los sistemas y datos del Gobierno de Aragón es fundamental para mantener la confianza pública y la eficacia operativa. En 2024, el Gobierno de Aragón se enfrenta a desafíos significativos que podrían comprometer la capacidad para funcionar de manera eficiente y segura.

FRAUDE EXTERNO

Descripción: Actores externos que pueden adoptar identidades falsas para influir en las operaciones o realizar actividades fraudulentas.

Impacto Potencial: Alteración de la precisión y veracidad de la información gestionada y publicada por el organismo.

FRAUDE INTERNO

Descripción: Riesgo de que empleados con acceso a sistemas críticos realicen acciones que podrían manipular o destruir datos.

Impacto Potencial: Compromisos en la toma de decisiones y pérdida de confianza interna y pública.

La protección de la integridad requiere un enfoque multidimensional que incluya tecnología, procesos y cultura organizacional. Es esencial para el Gobierno de Aragón implementar estrategias que protejan contra estos riesgos para mantener la operatividad y confianza de la ciudadanía. Para ello se van a tener en cuenta las siguientes consideraciones:

Prevención y Detección: Implementar soluciones de seguridad avanzadas y auditorías regulares para detectar y prevenir el acceso no autorizado y las manipulaciones, resaltando los esfuerzos en el desarrollo de los sistemas de control de acceso y gestión de permisos, para garantizar una correcta trazabilidad de las acciones que realizan los usuarios.

Cultura Organizacional: Fortalecer la cultura de integridad a través de la capacitación y políticas claras que desalienten y castiguen el comportamiento fraudulento.

PREVENIR Y GESTIONAR RIESGOS ACCIDENTALES

En el dinámico entorno tecnológico actual, los riesgos accidentales representan un desafío constante para la integridad y eficiencia operativa del Gobierno de Aragón. Estos riesgos, derivados de errores no intencionados o fallas sistémicas, pueden tener un impacto significativo en la capacidad para proporcionar servicios esenciales a la ciudadanía.

FALLO DE PROCEDIMIENTO

Descripción:
Errores humanos o malentendidos en la implementación de procedimientos operativos que pueden conducir a pérdidas de datos, operaciones incorrectas o mal uso de la tecnología.

Impacto Potencial:
Interrupciones operativas, pérdidas financieras y, en casos extremos, compromisos de seguridad que afectan a la ciudadanía

FALLO DE SUMINISTOS

Descripción:
Interrupciones o deficiencias en la provisión de suministros esenciales, como electricidad, servicios de red o componentes de hardware críticos.

Impacto Potencial:
Downtime de sistemas críticos, retrasos en la prestación de servicios y aumento del riesgo de pérdida de datos.

La gestión de riesgos accidentales es crucial para asegurar la estabilidad y confiabilidad de los servicios que el Gobierno de Aragón ofrece a la ciudadanía. Al fortalecer nuestras políticas de prevención y respuesta, podemos minimizar la probabilidad de incidentes y sus posibles impactos, para ello se potenciarán:

AUDITORÍAS REGULARES Y REVISIÓN DE PROCESOS

Implementar inspecciones y revisiones periódicas de todos los procedimientos y operaciones para identificar y corregir posibles puntos de fallo antes de que causen daño.

AUDITORÍAS REGULARES Y REVISIÓN DE PROCESOS

Capacitar a los empleados en mejores prácticas operativas y de seguridad para reducir la incidencia de errores humanos y aumentar la concienciación sobre los procedimientos correctos.

PLANES DE RESPUESTA ANTE EMERGENCIAS Y CONTINUIDAD DEL NEGOCIO

Desarrollar y mantener planes de contingencia robustos que permitan una rápida recuperación y continuidad de operaciones en caso de fallos accidentales significativos.

SALVAGUARDAR LA CONFIDENCIALIDAD

La confidencialidad es crucial para mantener la seguridad y la confianza pública en el Gobierno de Aragón. En un entorno donde las ciber amenazas son cada vez más sofisticadas, proteger la información sensible y privada se convierte en una prioridad máxima. La Administración de la Comunidad Autónoma se enfrenta a desafíos significativos que podrían comprometer su capacidad para proteger esta información vital.

RIESGOS DE CONFIDENCIALIDAD

ROBO DE INFORMACIÓN EXTERNA

Descripción: Extracción de datos confidenciales por actores externos a través de métodos como ciberataques, espionaje industrial o ciberdelincuencia.

Impacto Potencial: Compromiso de información clasificada, pérdida de confianza pública y riesgos de seguridad nacional.

ROBO DE INFORMACIÓN INTERNA

Descripción: Riesgo de divulgación no autorizada de información confidencial por parte de empleados, ya sea de manera intencional o accidental.

Impacto Potencial: Pérdida de ventaja competitiva, daño reputacional y posibles implicaciones legales por violación de la privacidad.

AMENAZAS

Phishing e Ingeniería Social: Tácticas cada vez más sofisticadas para engañar a los empleados y obtener acceso a información sensible.

Malware y Ransomware: Software malicioso que se introduce en los sistemas para robar o cifrar datos, exigiendo un rescate para su liberación.

Brechas de Datos en la Nube: Incidencias de seguridad en entornos de nube donde se almacena una gran cantidad de datos sensibles del organismo.

3 Objetivos estratégicos

OBJETIVOS ESTRATÉGICOS

Base para alcanzar los objetivos estratégicos

Los objetivos estratégicos se definen sobre unas bases ya establecidas en la doctrina de seguridad declarada en la política de Aragonesa de Servicios Telemáticos, en adelante AST. AST es una entidad de derecho público encargada de proporcionar servicios y soluciones de alto valor en el ámbito de las tecnologías y servicios de la información y telecomunicaciones al Gobierno de Aragón

Basándose en la doctrina de seguridad de la AST...

- Autonomía Operacional en Respuestas a Incidentes
- Defensa de la Autonomía Tecnológica
- Independencia en Análisis de Riesgos
- Regla del Décimo Hombre
- Alineación Interna
- Preparación ante Desastres
- Transparencia hacia el Usuario
- Eficiencia en la Gestión de Incidentes
- Minimización de la Superficie y Tiempo de Exposición

...Se busca cumplir los objetivos estratégicos

SECTOR PÚBLICO SEGURO

Fortaleciendo la infraestructura IT para diseñar y desplegar sistemas y procesos seguros y protegidos contra amenazas internas y externas.

SECTOR PÚBLICO VIGILANTE

Mejorando la detección y la inteligencia de amenazas para desarrollar la capacidad de anticipación de Aragón frente a ciberincidentes.

SECTOR PÚBLICO RESILIENTE

Garantizando una recuperación rápida ante incidentes, minimizando el impacto y manteniendo la continuidad de negocio.

OBJETIVOS ESTRATÉGICOS

Sector público seguro: Fortaleciendo la ciberseguridad en sistemas y procesos

El Gobierno de Aragón se enfrenta al desafío de **asegurar sus servicios TIC** ante un panorama de ciberamenazas en constante evolución, crecimiento y profesionalización. Por ello, se define como objetivo incrementar la colaboración con los entes y organismos con responsabilidad en este ámbito para garantizar su capacidad para **diseñar, desplegar y mantener sistemas y procesos robustos** que lo defiendan eficazmente contra cualquier intento de vulneración. Con esa meta en mente se plantean los siguientes objetivos, destinados a minimizar las vulnerabilidades y maximizar la ciberseguridad frente a amenazas tanto internas como externas:

FORTALECIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA

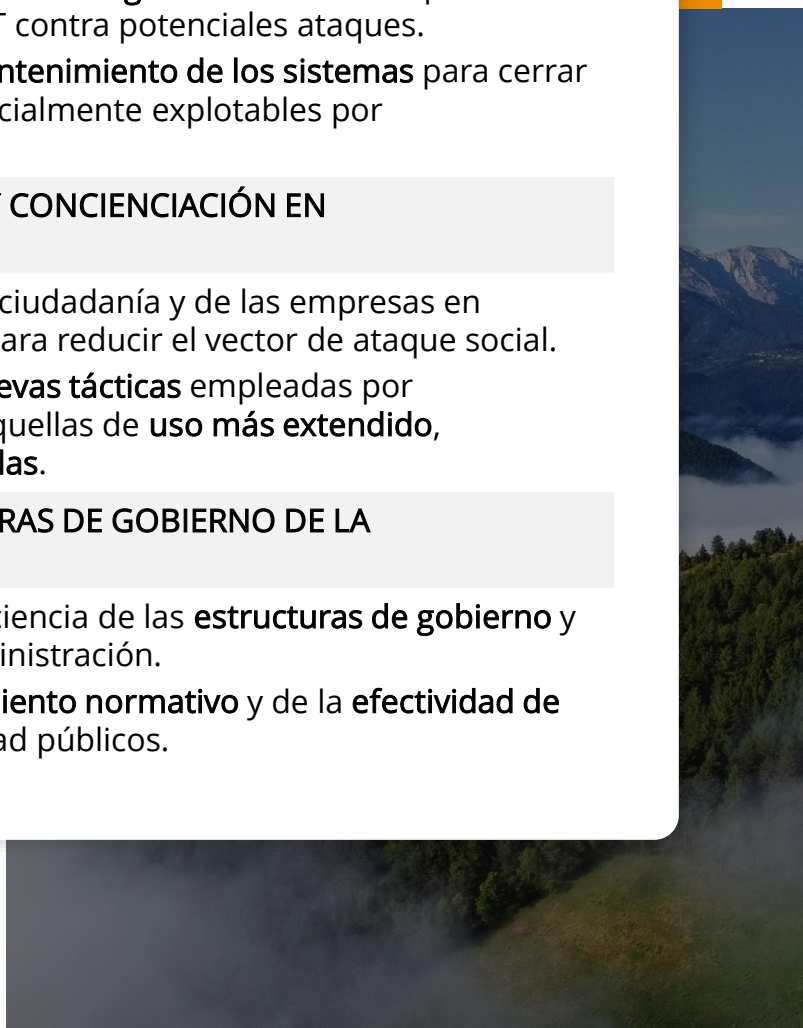
- Implementación de **soluciones de seguridad avanzadas** que protejan la infraestructura IT contra potenciales ataques.
- **Actualización continua** y **mantenimiento de los sistemas** para cerrar brechas de seguridad potencialmente explotables por ciberdelincuentes

MEJORA EN LA FORMACIÓN Y CONCIENCIACIÓN EN CIBERSEGURIDAD

- **Capacitación continua** de la ciudadanía y de las empresas en materia de ciberseguridad para reducir el vector de ataque social.
- Concienciación sobre las **nuevas tácticas** empleadas por ciberdelincuentes y sobre aquellas de **uso más extendido**, aprendiendo **cómo prevenirlas**.

REFUERZO DE LAS ESTRUCTURAS DE GOBIERNO DE LA CIBERSEGURIDAD

- Aumento en la eficacia y eficiencia de las **estructuras de gobierno** y **gestión del riesgo** de la administración.
- Aseguramiento del **cumplimiento normativo** y de la **efectividad de los equipos** de ciberseguridad públicos.



OBJETIVOS ESTRATÉGICOS

Sector público vigilante: Desarrollando estrategias de anticipación y respuesta ante incidentes

Como parte del compromiso con la seguridad, el Gobierno de Aragón desarrollará sus capacidades de vigilancia, fortaleciendo su habilidad para **anticiparse a potenciales incidentes** de forma eficaz, previniéndolos y evitando sus consecuencias. Mediante estas medidas no sólo se aumentará la protección contra ataques, sino que se **mantendrá la integridad de los servicios públicos digitales**, incrementando la confianza depositada en ellos. Por lo tanto, se pretende implementar un sistema integrado de vigilancia y detección proactiva de amenazas y anomalías mediante el cumplimiento de los siguientes objetivos:

IMPLEMENTACIÓN DE SISTEMAS DE DETECCIÓN AVANZADA

- Integración de **sistemas de monitorización** y **detección** de amenazas que identifiquen y respondan a tiempo real ante actividades anómalas.
- **Capacitación especializada** de los equipos de análisis de amenazas a través de formaciones técnicas.
- Preparación mediante la realización de **ejercicios de simulación de incidentes** para su identificación rápida y precisa.

FORTALECIMIENTO DE LA INTELIGENCIA DE AMENAZAS

- Establecimiento de **colaboraciones estratégicas** con otras entidades gubernamentales y privadas para el intercambio de inteligencia de amenazas y mejores prácticas del sector, mejorando la capacidad de anticipación y respuesta.
- **Recopilación y análisis de información** sobre nuevas vulnerabilidades, técnicas de ataque y otras afectaciones a la administración mediante el uso de plataformas de inteligencia de amenazas.

OBJETIVOS ESTRATÉGICOS

Sector público resiliente: Formulando estrategias de recuperación y continuidad ante incidentes

Pese a que la situación ideal desde un punto de vista de ciberseguridad es evitar y prevenir todos los ataques mediante el establecimiento de medidas de securización de la información y los sistemas, no siempre es posible evitar y bloquear todos los intentos de vulneración. Es por ello por lo que resulta crucial trabajar en mejorar la resiliencia, garantizando la **capacidad de recuperación y la continuidad de las operaciones** tras un incidente de ciberseguridad. La finalidad es garantizar el desarrollo de las actividades esenciales, mejorando la confianza pública y minimizando el impacto en los servicios y en la infraestructura crítica, asegurando:

DESARROLLO DEL PLAN DE CONTINUIDAD

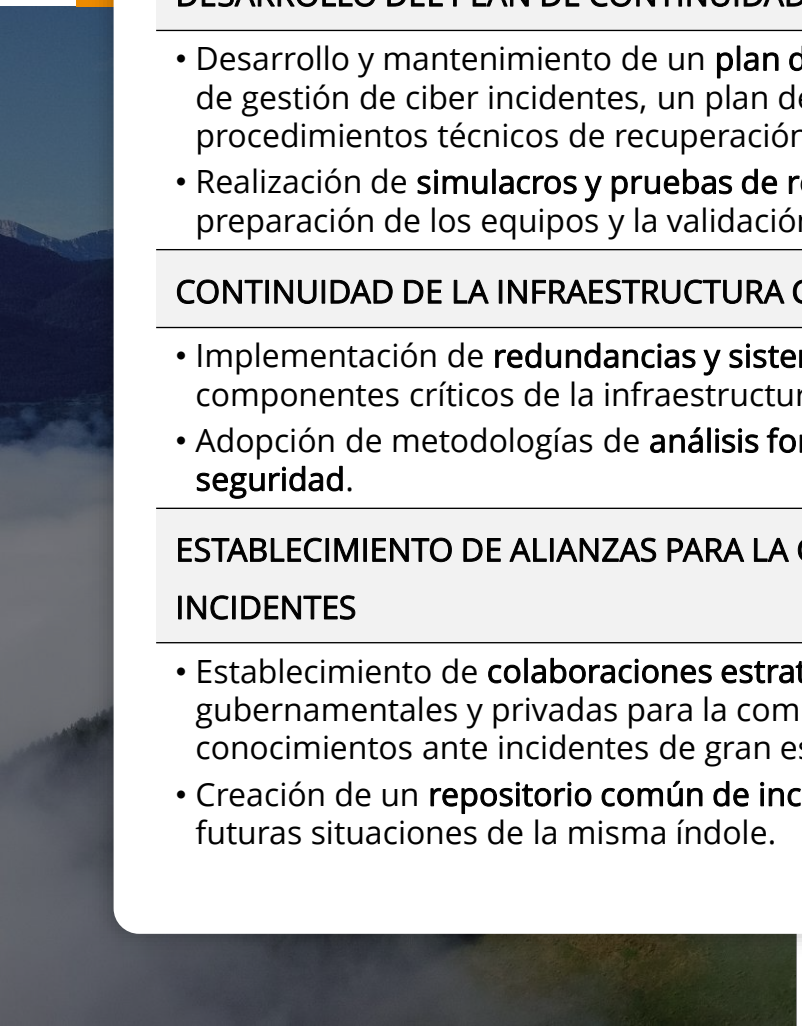
- Desarrollo y mantenimiento de un **plan de continuidad**, incluyendo un plan de gestión de ciber incidentes, un plan de recuperación ante desastres y los procedimientos técnicos de recuperación asociados.
- Realización de **simulacros y pruebas de recuperación** regulares para la preparación de los equipos y la validación y mejora continua de los planes.

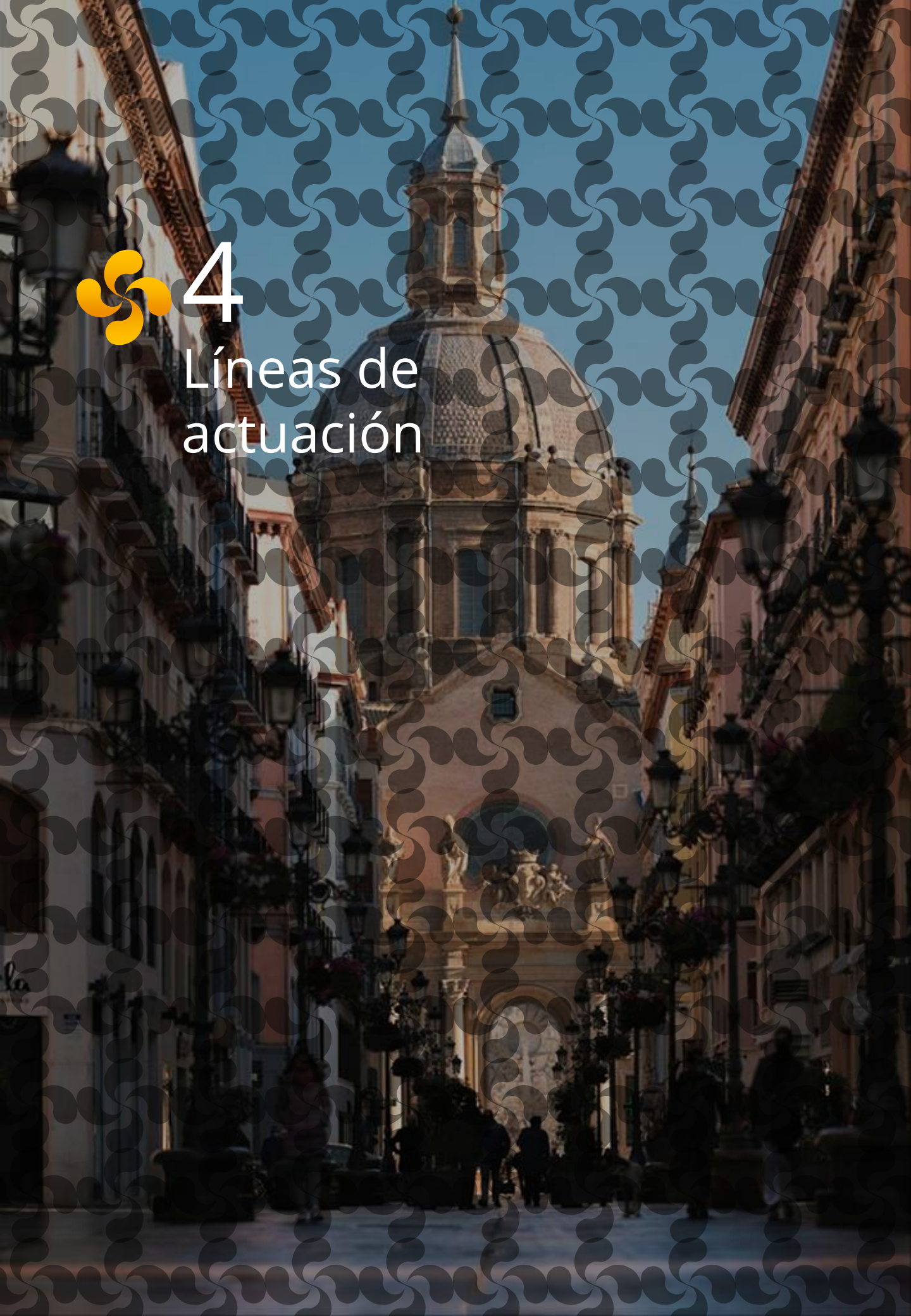
CONTINUIDAD DE LA INFRAESTRUCTURA CRÍTICA

- Implementación de **redundancias y sistemas de failover** para los componentes críticos de la infraestructura.
- Adopción de metodologías de **análisis forense** y de realización de **copias de seguridad**.

ESTABLECIMIENTO DE ALIANZAS PARA LA GESTIÓN Y RECUPERACIÓN ANTE INCIDENTES

- Establecimiento de **colaboraciones estratégicas** con otras entidades gubernamentales y privadas para la compartición de recursos y conocimientos ante incidentes de gran escala o con afectación transversal.
- Creación de un **repositorio común de incidentes** para su consulta ante futuras situaciones de la misma índole.





4
Líneas de actuación

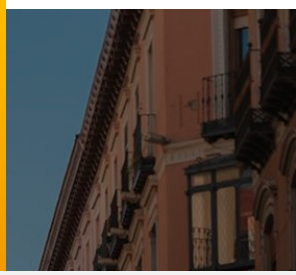
LÍNEAS DE ACTUACIÓN

Centralización y coordinación de la estrategia de ciberseguridad

El Gobierno de Aragón establece el **Centro de Ciberseguridad de Aragón (CCA)** como respuesta a la creciente necesidad de una **gestión eficiente de la ciberseguridad** dentro del sector público. Este centro sirve como núcleo para la **coordinación y ejecución** de las actividades relacionadas con la ciberseguridad en la administración pública, con el objetivo de fortalecer la protección contra ciber amenazas y asegurar la continuidad y eficacia de los servicios públicos.

ÁMBITOS DE ACTUACIÓN DEL CENTRO DE CIBERSEGURIDAD DE ARAGÓN (CCA)

- Excelencia en ciberseguridad
- Operaciones de seguridad
- Respuesta a ciber incidentes



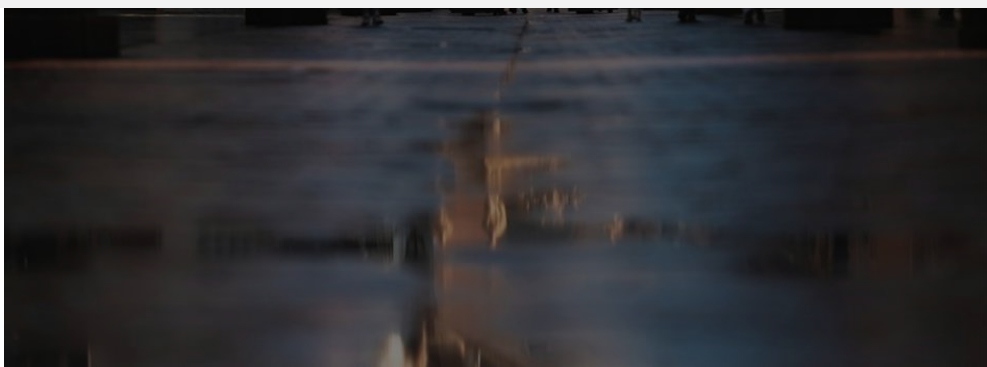
PILARES BÁSICOS DEL CENTRO DE CIBERSEGURIDAD DE ARAGÓN (CCA)

COORDINACIÓN DE ESTRATEGIAS

Centralizar las capacidades de ciberseguridad del Gobierno de Aragón para desarrollar y ejecutar la estrategia de ciberseguridad de manera unificada.

COLABORACIÓN SECTORIAL

Facilitar la colaboración entre diferentes entidades del sector público mediante convenios que permitan el acceso a servicios especializados de ciberseguridad.



LÍNEAS DE ACTUACIÓN

Centralización y coordinación de la estrategia de ciberseguridad

El Gobierno de Aragón establece el **Centro de Ciberseguridad de Aragón (CCA)** como respuesta a la creciente necesidad de una **gestión eficiente de la ciberseguridad** dentro del sector público. Este centro sirve como núcleo para la **coordinación y ejecución** de las actividades relacionadas con la ciberseguridad, con el objetivo de fortalecer la protección contra ciberamenazas y asegurar la continuidad y eficacia de los servicios públicos.

CAPACIDADES TRANSVERSALES DEL CENTRO DE CIBERSEGURIDAD DE ARAGÓN

POTENCIAR LA CIBERSEGURIDAD EN EL TERRITORIO DE ARAGÓN

- Asegurar la integridad de las redes de comunicaciones electrónicas y los sistemas de información del Gobierno de Aragón.
- Ejecutar políticas públicas que refuercen la ciberseguridad en toda la región.

ASESORAMIENTO Y APOYO EN LA PLANIFICACIÓN

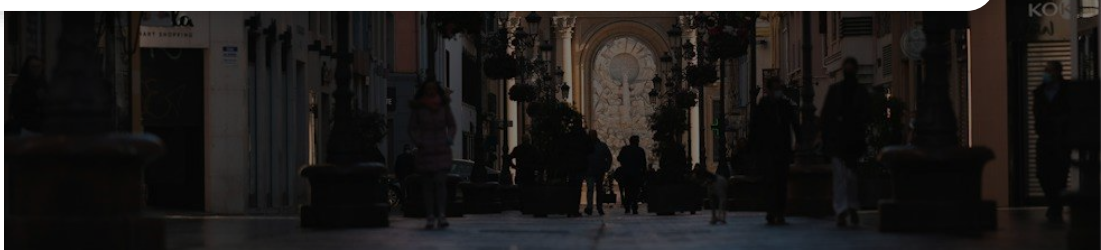
- Proveer asesoría continua al Gobierno de Aragón en la elaboración y aprobación de planes de ciberseguridad.
- Supervisar y ejecutar los planes de ciberseguridad vigentes para cumplir con los objetivos estratégicos establecidos.

EDUCACIÓN Y CONCIENCIACIÓN

- Organizar actividades de formación y sensibilización en ciberseguridad, con un enfoque particular en colectivos vulnerables.
- Desarrollar y distribuir herramientas y programas educativos para fortalecer la cultura de seguridad en todo el sector público.

COORDINACIÓN CON OTROS ORGANISMOS

- Establecer alianzas estratégicas con otros organismos y entidades para mejorar la capacidad de respuesta y prevención frente a ciberincidentes.



LÍNEAS DE ACTUACIÓN

Siguiendo nuestros principios para alcanzar los objetivos estratégicos

Una vez establecidos los objetivos... ...Definimos líneas de actuación para alcanzarlos

SECTOR PÚBLICO
SEGURO

SECTOR PÚBLICO
VIGILANTE

SECTOR PÚBLICO
RESILIENTE

CENTRO DE CIBERSEGURIDAD DE ARAGÓN (CCA)

GOBIERNO DE ARAGON

Fortalecimiento tecnológico

Promover la mejora de las condiciones de ciberseguridad del sector privado

Cultura en materia de ciberseguridad

SOC en colaboración y coordinación con entidades para extender la protección

Capacidades de prevención, detección y respuesta a incidentes

LÍNEAS DE ACTUACIÓN

Fortalecimiento tecnológico

Cumplimiento normativo y coordinación	• Asegurar que todas las plataformas tecnológicas cumplen con las regulaciones vigentes para la protección de datos. • Coordinar las acciones de cumplimiento normativo a través de todas las entidades dentro de la administración para garantizar una respuesta unificada y eficiente para todas las entidades.
Especialización del personal técnico	• Fortalecer las capacidades del personal técnico mediante formación especializada en ciberseguridad, asegurando que están preparados para manejar y a los desafíos actuales y emergentes de ciberseguridad.
Impulsar el protagonismo del centro de ciberseguridad	• Desarrollar el Centro de Ciberseguridad de Aragón pensado como la pieza clave que actúe como el núcleo central para la gestión de la ciberseguridad en la Comunidad Autónoma de Aragón, coordinando recursos, capacidades y estrategias para una defensa efectiva.
Aplicación de Security by Design	• Integrar principios de ciberseguridad en el diseño y desarrollo de todos los sistemas y servicios, promoviendo prácticas seguras que prevengan vulnerabilidades desde la fase inicial.
Definir estructuras organizativas especializadas	• Definir claramente las estructuras organizativas que se especializarán en ciberseguridad, estableciendo perfiles y responsabilidades claras para facilitar la implementación efectiva de estrategias de seguridad.

LÍNEAS DE ACTUACIÓN

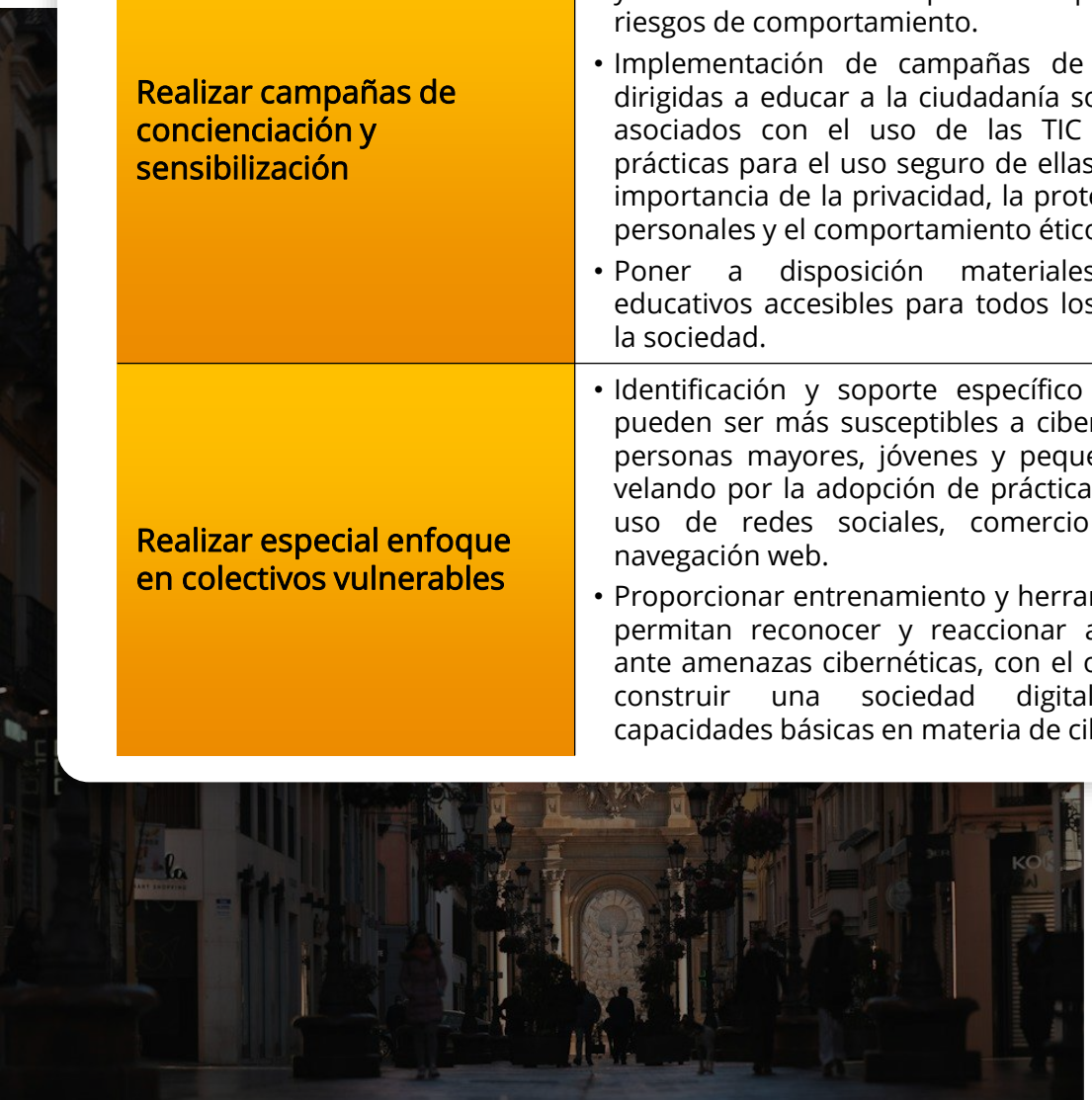
Promover la mejora de las condiciones de ciberseguridad del sector privado

Promover la colaboración multisectorial	• Fomentar la colaboración entre entidades e instituciones públicas y privadas especializadas en ciberseguridad a nivel nacional e internacional. • Establecer conexiones con el CNPIC, empresas TIC, y organismos competentes en ciberseguridad como el Centro Criptológico Nacional. Desde su creación en el año 2007, el CNPIC ha establecido una compleja comunidad de seguridad, formada por más de 250 operadores críticos, de carácter público-privado.
Reforzar los mecanismos de alerta temprana y prevención	• Reforzar los sistemas de alerta temprana para detectar amenazas emergentes de forma más eficiente. • Implementar herramientas específicas que mejoren los procesos de notificación y compartido de información con relación a amenazas y vulnerabilidades.
Desarrollo de talento calificado en ciberseguridad	• Abordar la brecha existente entre la demanda y la oferta de perfiles técnicos y jurídicos especializados mediante programas educativos atractivos. • Potenciar las prácticas profesionales y la formación continua para preparar a los futuros profesionales del sector, aumentando la disponibilidad de expertos en ciberseguridad.
Crear el mapa de actores clave en ciberseguridad	• Identificar y establecer relaciones con los actores clave en el ámbito de la ciberseguridad, tanto a nivel nacional como internacional. • Asegurar una cooperación efectiva entre todos los stakeholders para una respuesta coordinada ante incidentes.

LÍNEAS DE ACTUACIÓN

Cultura en materia de ciberseguridad

Desarrollo de iniciativas basadas en la evaluación de riesgos de comportamiento	• Mejorar la seguridad a través de un nuevo plan basado en el conocimiento de las conductas y/o comportamientos de las personas. • Definir un modelo práctico, estructurado y eficaz que permita evaluar, medir y monitorizar la madurez de concienciación en ciberseguridad de las personas. • En el ámbito de la Administración de la Comunidad Autónoma de Aragón, enfocar el plan a diferentes riesgos según el puesto de trabajo, realizando campañas no solo a nivel global, sino adaptadas a cada puesto de trabajo y a los diferentes niveles de madurez de los empleados y su capacidad de aprendizaje.
Realizar campañas de concienciación y sensibilización	• Ofrecer contenidos innovadores de gran calidad potenciando módulos interactivos de corta duración y basados en casos prácticos que representen riesgos de comportamiento. • Implementación de campañas de concienciación dirigidas a educar a la ciudadanía sobre los riesgos asociados con el uso de las TIC y las mejores prácticas para el uso seguro de ellas, destacando la importancia de la privacidad, la protección de datos personales y el comportamiento ético. • Poner a disposición materiales y recursos educativos accesibles para todos los segmentos de la sociedad.
Realizar especial enfoque en colectivos vulnerables	• Identificación y soporte específico a grupos que pueden ser más susceptibles a ciberataques, como personas mayores, jóvenes y pequeñas empresas, velando por la adopción de prácticas seguras en el uso de redes sociales, comercio electrónico y navegación web. • Proporcionar entrenamiento y herramientas que les permitan reconocer y reaccionar adecuadamente ante amenazas cibernéticas, con el objetivo final de construir una sociedad digital plena con capacidades básicas en materia de ciberseguridad.



LÍNEAS DE ACTUACIÓN

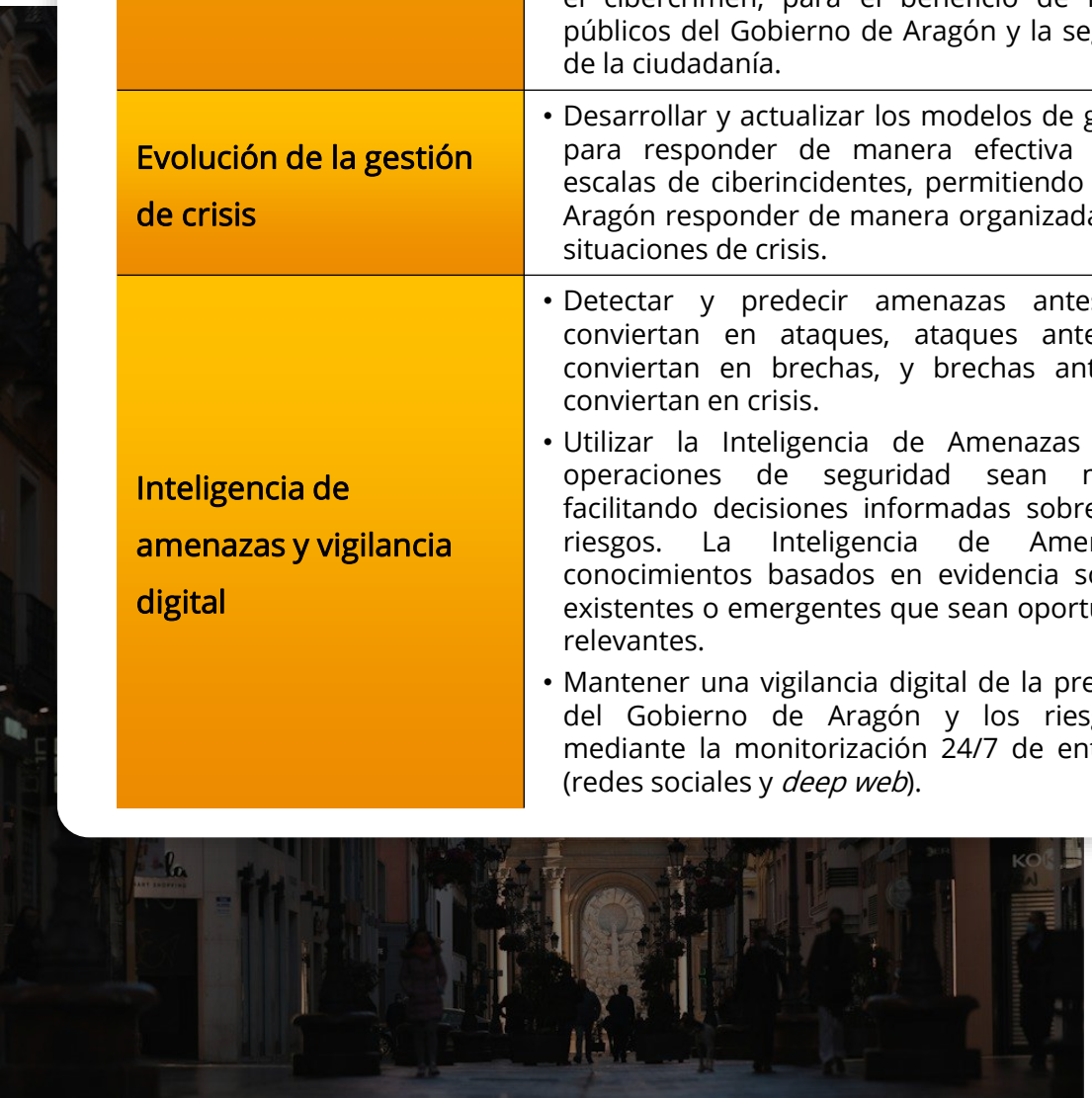
SOC en colaboración y coordinación con entidades para extender la protección

Promoción de la colaboración con otras entidades	• Promover la colaboración y coordinación con entidades e instituciones públicas y privadas, tanto nacionales como internacionales, especializadas en materia de ciberseguridad. • Reforzar los mecanismos de alerta temprana de amenazas y de prevención de incidentes, a través del uso de herramientas específicas de notificación y compartición de datos, contribuyendo a la mejora del nivel de ciberseguridad y de las capacidades de protección del conjunto de entidades de la Administración autonómica, como del ámbito local, diputaciones provinciales, ayuntamientos y otros entes públicos.
Estímulo al crecimiento de la Industria de ciberseguridad	• Apoyar la creación y desarrollo de empresas especializadas en ciberseguridad, fomentando la innovación y la investigación. • Promover la colaboración con centros universitarios y de investigación para trasladar conocimientos y desarrollos tecnológicos al mercado.
Inclusión de activos de seguridad en la Red Nacional de SOC	• Potenciar la presencia de los activos de seguridad aragoneses en la red nacional de SOCs, generando sinergias entre organismos. • Ampliar la coordinación y la cooperación entre el sector público y privado, así como con los organismos competentes en materia de ciberseguridad (Centro Criptológico Nacional).

LÍNEAS DE ACTUACIÓN

Capacidades de prevención, detección y respuesta a incidentes

Fortalecimiento del CSIRT	• Reforzar el Equipo de Respuesta (CSIRT) con recursos adicionales, expandiendo sus servicios y ámbito de actuación, estando al servicio de organismos públicos del Gobierno de Aragón. • Mejorar las herramientas tecnológicas utilizadas por el CSIRT para agilizar la detección y contención de amenazas cibernéticas.
Coordinación con fuerzas de seguridad	• Intensificar la colaboración con las fuerzas y cuerpos de seguridad del estado para fortalecer las estrategias de prevención y gestión. • Comunicación con el resto de CSIRT nacionales de referencia y la Secretaría de Estado de Seguridad del Ministerio del Interior a través de Oficina de Coordinación de Ciberseguridad (OCC). • Reenfocar los acuerdos de colaboración para facilitar un enfoque más proactivo y coordinado en la lucha contra el cibercrimen, para el beneficio de los organismos públicos del Gobierno de Aragón y la seguridad pública de la ciudadanía.
Evolución de la gestión de crisis	• Desarrollar y actualizar los modelos de gestión de crisis para responder de manera efectiva a las diversas escalas de ciberincidentes, permitiendo al Gobierno de Aragón responder de manera organizada y resiliente en situaciones de crisis.
Inteligencia de amenazas y vigilancia digital	• Detectar y predecir amenazas antes de que se conviertan en ataques, ataques antes de que se conviertan en brechas, y brechas antes de que se conviertan en crisis. • Utilizar la Inteligencia de Amenazas para que las operaciones de seguridad sean más eficientes facilitando decisiones informadas sobre la gestión de riesgos. La Inteligencia de Amenazas implica conocimientos basados en evidencia sobre amenazas existentes o emergentes que sean oportunas, precisas y relevantes. • Mantener una vigilancia digital de la presencia en línea del Gobierno de Aragón y los riesgos relevantes mediante la monitorización 24/7 de entornos digitales (redes sociales y *deep web*).




GOBIERNO
DE ARAGON