GOBIERNO DEL ESTADO
2022|2027

AGENCIA DE TRANSFORMACIÓN DIGITAL DEL ESTADO DE QUINTANA ROO

Guía de Ciberseguridad para la Administración Pública Estatal

Índice

Introducción

El presente documento tiene por objeto establecer una guía de referencia para los Sujetos Obligados de la Administración Pública Estatal en materia de ciberseguridad, mediante la definición de objetivos estratégicos, líneas de acción y actividades orientadas a fortalecer las capacidades institucionales para la protección de la información, los sistemas tecnológicos y los servicios digitales gubernamentales.

En un entorno digital caracterizado por riesgos y amenazas cibernéticas cada vez más complejas y sofisticadas, resulta indispensable impulsar mecanismos coordinados que permitan consolidar una cultura de ciberseguridad en las dependencias y entidades de la Administración Pública Estatal, promoviendo la adopción de buenas prácticas, lineamientos técnicos y esquemas de colaboración interinstitucional.

En este contexto, el presente instrumento busca fortalecer las capacidades de prevención, detección, atención y mitigación de incidentes de ciberseguridad, mediante una coordinación estratégica con la ATD, así como fomentar el desarrollo de competencias técnicas especializadas en los servidores públicos responsables de las Tecnologías de la Información y Comunicaciones (TIC).

Asimismo, se propone impulsar acciones permanentes de capacitación, talleres, cursos y certificaciones especializadas en materia de ciberseguridad, orientadas tanto al personal técnico como a las y los servidores públicos en general, con la finalidad de promover conocimientos básicos de seguridad digital, fortalecer la concientización institucional y contribuir a la protección integral del ecosistema tecnológico gubernamental.

Marco normativo

Constitución Política de los Estados Unidos Mexicanos.

Esta guía establece las bases de ciberseguridad en la Administración Pública Estatal, en seguimiento al derecho a la protección de los datos personales y como parte de los esfuerzos de la ATD para fortalecer las capacidades tecnológicas pública en apego al Artículo 16, sección II y el Artículo 25 , sección última de la Constitución Política de los Estados Unidos Mexicanos.

Ley Nacional para Eliminar Trámites Burocráticos.

La Ley Nacional para Eliminar Trámites Burocráticos, establece en su artículo 6, fracción XIII a la ciberseguridad como uno de los principios que deben observar los Sujetos Obligados en el cumplimiento de sus obligaciones en materia de simplificación administrativa, digitalización de trámites y servicios y fortalecimiento de capacidades tecnológicas públicas. Asimismo, el artículo 25, fracciones V y VI, prevé la observancia de estándares de seguridad y mecanismos de actualización tecnológica para la digitalización de trámites y servicios.

La presente guía se emite en cumplimiento a las atribuciones conferidas en el Artículo 13, fracción XVII, como apoyo y acompañamiento a los Sujetos Obligados en la recepción, implementación y actualización de las soluciones tecnológicas, siguiendo el principio de ciberseguridad establecido en la ley.

Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Quintana Roo

La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados, define la obligación del Estado por garantizar la privacidad de los individuos y velar por que no se incurran en conductas que afecten arbitrariamente a los individuos con su información como lo menciona en el Artículo 8 de la Ley.

Con el objetivo de proteger los datos personales de los individuos, se emiten recomendaciones para la protección del ecosistema de Tecnologías de los Sujetos Obligados de la Administración Pública Estatal como medida preventiva.

Plan Estatal de Desarrollo 2023-2027.

El Plan Estatal de Desarrollo 2023 - 2027 es un documento que define las prioridades del Estado para cubrir las necesidades de la ciudadanía. En el tema 5.24 Transparencia y Combate a la Corrupción, en la línea de acción 5.24.3.7 se especifica "Promover la ciberseguridad al interior de las diferentes instancias gubernamentales del Estado mediante la promoción de políticas, mecanismos de prevención y protocolos de respuesta ante incidentes digitales y cibernéticos."

Decreto de Creación de la Agencia de Transformación Digital

La Agencia de Transformación Digital del Estado de Quintana Roo, como Autoridad Estatal de Simplificación y Digitalización, cuenta con la facultad para diseñar e implementar políticas públicas en materia TIC, establecer políticas y lineamientos para la gestión y administración de los Centros de Datos de los Sujetos Obligados y proponer lineamientos y estándares, para fortalecer, modernizar y armonizar los sistemas tecnológicos de la Administración Pública Estatal, como se establece en el Artículo 6, sección II, V y VI.

En consecuencia, la Agencia de Transformación Digital, desarrolla el presente documento, como guía para la protección del ecosistema tecnológico de los Sujetos Obligados de la Administración Pública Estatal y evitar las brechas de seguridad de las TIC.

Glosario, Siglas y Acrónimos

ATD: Agencia de Transformación Digital del Estado de Quintana Roo.

Ciberseguridad: Conjunto de estrategias, procesos, regulación, normas técnicas, controles, herramientas y acciones de cultura y concientización orientadas a proteger los activos, incluyendo la infraestructura tecnológica, redes, sistemas de información, base de datos, datos personales, instalaciones y todo componente en el que se recaba, convierte, almacena, protege, procesa, transmite, usa y recupera información dentro de la Administración Pública Estatal.

Cibercrimen: El cibercrimen es una actividad delictiva que se dirige a una computadora, una red informática o un dispositivo en red, o bien que utiliza uno de estos elementos.

CIS Controls: Conjunto de mejores prácticas y directrices de ciberseguridad desarrolladas por el Centro para la Seguridad de Internet (CIS) que ayudan a las organizaciones a protegerse contra las amenazas cibernéticas más comunes.

Continuidad: Implementación de acciones preventivas, para mitigación y de recuperación en caso de una interrupción.

Disponibilidad: Propiedad de la información que garantiza que la información estará accesible en el momento que las personas autorizadas lo requieran.

DevSecOps: Desarrollo, Seguridad y Operaciones, es la integración de seguridad informática en cada etapa del ciclo de vida del software.

Darknet: Es una red privada superpuesta a Internet, diseñada para mantener el anonimato y la privacidad.

DNS: Sistema de Nombres de Dominio.

EDR/XDR: Herramientas para detectar, investigar y responder a amenazas en dispositivos y redes (Endpoint/Extended Detection and Response).

Endpoints: Dispositivos finales conectados a la red, como computadoras, móviles o servidores.

Identidad y Accesos (IAM): Gestión de usuarios, permisos y autenticación para asegurar el acceso adecuado a recursos.

Normas ISO: Organización Internacional de Estándares (ISO por sus siglas en inglés)

IA: Inteligencia Artificial

ISP: Internet Service Provider.

Phishing: Técnica de ingeniería social en la que se suplanta la identidad de fuentes de confianza para robar información.

TI: Tecnologías de Información

Typosquatting: Es una técnica de fraude cibernético en la que los atacantes registran nombres de dominio web que son similares a marcas o sitios web legítimos, aprovechando errores de escritura comunes.

Múltiple Factor de Autenticación (MFA): Método de seguridad que exige dos o más pruebas de identidad para acceder a un sistema.

Plan de Continuidad Operativa (PCO): Estrategia para mantener funciones críticas durante interrupciones.

Plan de Recuperación ante Desastres (DRP): Plan para restaurar sistemas y operaciones tras un evento catastrófico.

Respaldos: Copias de seguridad de datos que permiten recuperarlos en caso de pérdida, daño o ataque.

Riesgo: Potencial de que una amenaza explote las vulnerabilidades de un activo.

Soluciones Tecnológicas: los sistemas tecnológicos, plataformas, aplicaciones web, aplicaciones móviles o similares y, en general, cualquier programa de cómputo.

Sujetos Obligados: las dependencias, órganos administrativos desconcentrados y entidades paraestatales de la Administración Estatal.

TIC: Tecnologías de la Información y Comunicación.

Vulnerabilidad: Factor de riesgo de un componente o sistema que está susceptible a sufrir un daño.

Zero Trust: Modelo de seguridad basado en “nunca confiar, siempre verificar”, que asume que ninguna persona o dispositivo dentro o fuera de la red de una organización debe tener acceso por defecto, sino que requiere una validación explícita en cada solicitud de acceso.

Justificación

En los últimos años, el volumen e intensidad de los intentos de ciberataques dirigidos contra personas, empresas, infraestructuras y sujetos obligados han crecido de manera exponencial, evidenciando un entorno digital cada vez más hostil y sofisticado. Este incremento representa una amenaza real para la continuidad de los servicios públicos estatales, la seguridad de la información gubernamental y la confianza de la ciudadanía y del sector turístico en los entornos digitales.

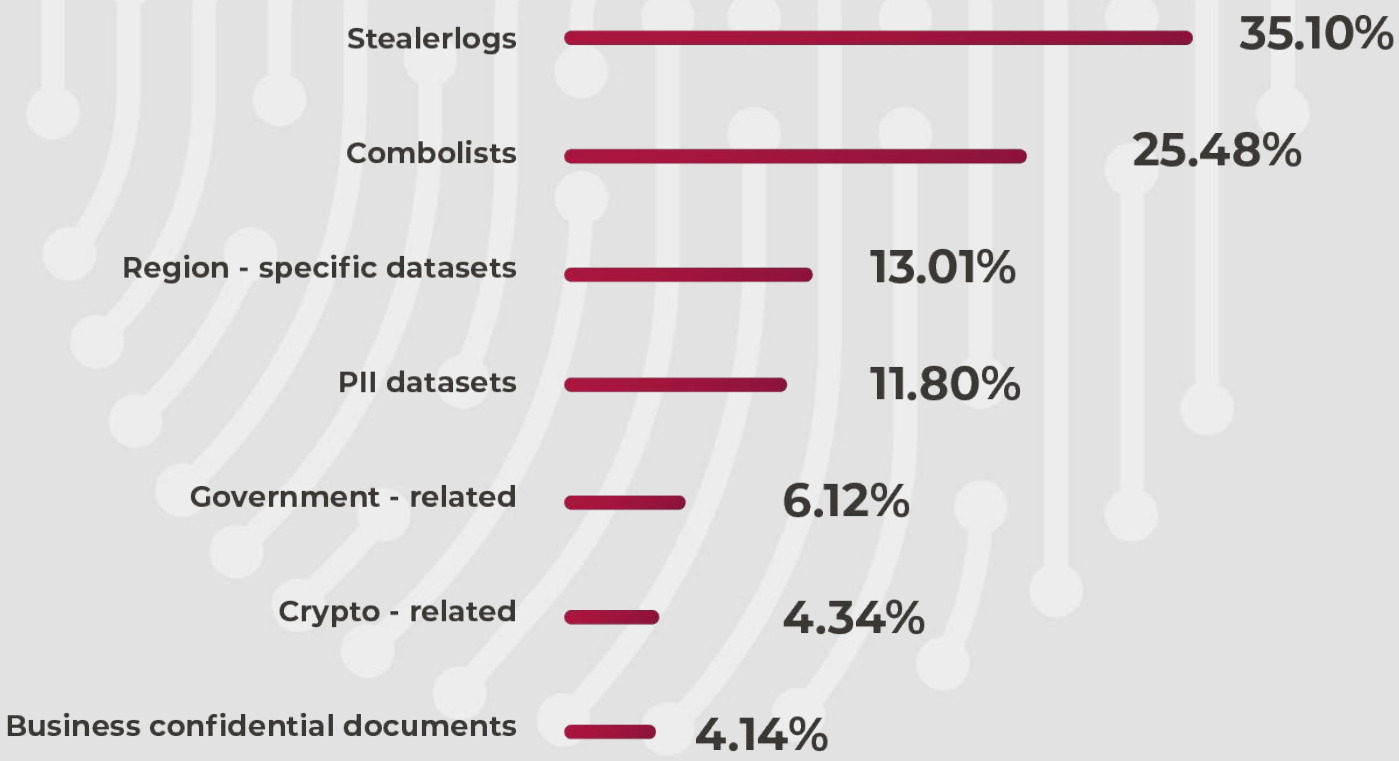
El Estado de Quintana Roo, por su alta concentración turística, tiene un volumen significativo de transacciones digitales, intercambio de datos personales y operaciones financieras. Este contexto lo convierte en un objetivo estratégico para actores maliciosos que buscan explotar vulnerabilidades mediante fraudes electrónicos, robo de identidad, campañas de phishing y ataques a sistemas críticos.

Tomando en cuenta esto, ninguna institución pública estatal, empresa del sector turístico, ni organización privada está exenta de enfrentar ciberataques. La interconexión de los ecosistemas digitales genera efectos en cadena que pueden impactar directa o indirectamente a individuos, familias, empresas y a las instituciones públicas del estado.

La modernización administrativa y los proyectos de innovación digital impulsados por el Gobierno del Estado sólo serán sostenibles si se acompañan de un fortalecimiento integral de la ciberseguridad, capaz de garantizar confianza, resiliencia y continuidad operativa en los servicios públicos, particularmente en áreas críticas como seguridad pública, recaudación, salud y turismo.

La administración pública estatal interactúa con proveedores tecnológicos, plataformas digitales, operadores turísticos, instituciones financieras y usuarios nacionales e internacionales. En este contexto, resulta indispensable adoptar un enfoque de gestión basado en riesgos que contemple toda la cadena de valor, es decir, la red de actores, procesos, infraestructura e información que conforman el ecosistema digital del estado.

En los últimos años, se han detectado grandes aumentos de ataques, según el *Fortinet Global Threat Landscape Report 2026,* el cibercrimen ha operado como un sistema industrial en lugar de un conjunto de campañas aisladas, registrando un total de 640 billones de eventos de reconocimiento en 2025. En este mismo año, la base de datos de la Darknet estuvo dominada por conjuntos de datos utilizados y optimizados para la automatización de ataques, no solo para la explotación de vulnerabilidades puntuales. El 6.12% de estos datos son de instituciones gubernamentales, demostrando que, con esta información y el uso de IA, permite reducir el tiempo para automatizar el acceso inicial a los sistemas y plataformas gubernamentales. (Fortinet, Inc. 2026)



Fortinet Inc / Darknet database offerings 2025/ 2026/ Fortinet,com/ . - https://www.fortinet.com/lat/resources/reports/threat-landscape-report

Principios de ciberseguridad

Los principios aplicables a la administración pública estatal orientan la ejecución y seguimiento de las acciones que se deberán de desarrollar para el cumplimiento de los objetivos y el alcance del presente documento. Estos principios deberán implementarse como un componente fundamental para la creación de estrategias, según corresponda en el desarrollo de toda acción, proyecto y estrategia que pueda estar relacionado con la ciberseguridad.

1. **Ciberseguridad como valor público**

   La ciberseguridad protege la confidencialidad, integridad y disponibilidad para que los servicios públicos se mantengan resilientes, activos y accesibles, para que los datos no se expongan o se modifiquen por entes externos y la ciudadanía confíe en el uso de las herramientas tecnológicas que se ponen a su disposición por la administración pública estatal.

2. **Ciberseguridad por diseño**

   Todo proyecto que implique el uso, desarrollo o intervención de tecnologías en el Estado de Quintana Roo deberá incorporar la ciberseguridad como un eje transversal desde su fase de planeación, implementación, operación y cierre.

3. **Responsabilidad Institucional**

   Las instituciones que integran la Administración Pública del Estado de Quintana Roo son responsables de la gestión de sus riesgos y de la protección de sus activos de información, infraestructura tecnológica y servicios digitales, por lo que no está acotada a las áreas de tecnología, ciberseguridad o afines.

4. Ciberseguridad como valor público

Los Sujetos Obligados, deberán diseñar, implementar, mantener y actualizar de manera continua un Plan de Prevención, Respuesta y Recuperación ante Incidentes de Seguridad de la Información y Ciberseguridad.

Se deberá priorizar en todo momento la continuidad operativa de los servicios públicos críticos, así como la identificación, registro y resguardo de evidencias digitales que permitan el análisis forense, la trazabilidad de los incidentes y, en su caso, la atención de responsabilidades administrativas o legales conforme al marco normativo aplicable.

5. Gestión del Riesgo

El riesgo en materia de seguridad de la información y ciberseguridad es inherente a la operación de las instituciones públicas y evoluciona de manera constante, en función de los cambios tecnológicos, regulatorios y del entorno digital.

Es indispensable establecer mecanismos permanentes de evaluación y gestión de riesgos, que permitan identificar, analizar y monitorear de forma continua las amenazas y vulnerabilidades. Deberán ajustar de manera dinámica los controles de seguridad existentes, así como implementar medidas adicionales que resulten necesarias para mitigar los riesgos de forma efectiva.

6. Adecuación Tecnológica

Los Sujetos Obligados presentan particularidades y niveles de seguridad distintos. Es fundamental evaluar y adaptar la normatividad vigente, priorizando la protección de la infraestructura, las comunicaciones y la información, y asegurando una evolución continua que permita implementar los controles de seguridad necesarios.

7. **Innovación**

Actualizar las capacidades en tecnología y operación en planes estructurados y detallados, no solamente desde la perspectiva de ciberseguridad, sino del conjunto de tecnologías obsoletas que incrementan la exposición a vulnerabilidades.

8. **Respeto a los derechos humanos en el entorno digital**

El ecosistema de ciberseguridad debe orientarse a garantizar los derechos de la ciudadanía, priorizando la soberanía de los datos individuales, la privacidad, la protección de la información, la libertad de expresión y el acceso pleno a la información presentada y relevante para el uso de sus datos..

Alcance

Sujetos Obligados

La presente guía es de observancia para las dependencias, órganos administrativos desconcentrados y entidades paraestatales de la Administración Estatal.

Áreas o unidades responsables

Cada dependencia, sus órganos administrativos desconcentrados y entidades de la Administración Pública Estatal deberán contar con un área o unidad responsable de la ciberseguridad, con un titular encargado de la aplicación de la Política de Ciberseguridad.

Funcional

Estos principios se aplicarán a todas las actividades, personas, procesos, servicios, tecnologías, sistemas de información y/o activos digitales que:

I. Apoyen el cumplimiento de funciones sustantivas y administrativas de los Sujetos Obligados.
II. Involucre el tratamiento, almacenamiento, transmisión o protección de información de cualquier tipo.
III. Están relacionados con la prestación de servicios digitales a la población y/o a los Sujetos Obligados.
IV. Son parte de redes, plataformas, nubes o infraestructuras tecnológicas utilizadas, gestionadas y operadas por los Sujetos Obligados.

Objetivo General

Establecer las bases, principios, lineamientos y mecanismos institucionales en materia de ciberseguridad para las dependencias y entidades de la Administración Pública Estatal, a fin de fortalecer la protección de los activos de información, garantizar la continuidad operativa de los servicios públicos, salvaguardar los datos personales y sensibles, y mitigar los riesgos derivados del entorno digital.

Ejes estratégicos y objetivos específicos

Los ejes estratégicos y sus actividades, podrán ser implementadas de manera progresiva para lograr los objetivos descritos de manera gradual, hasta su completa implementación por los Sujetos Obligados de la Administración Pública Estatal.

Eje 1: Gobernanza de datos y cumplimiento

La ciberseguridad en la Administración Pública Estatal requiere de un marco normativo homogéneo y de mecanismos de coordinación institucional que aseguren la correcta aplicación de estándares técnicos. Este marco integral se elaborará tomando como referencia las buenas prácticas internacionales e incorporará reglas claras, simples y medibles, diseñadas para ser adoptadas en el corto plazo,

garantizando consistencia y aplicabilidad en toda la Administración Pública Estatal.

Se promoverá la creación de catálogos de controles mínimos, que consideren el ecosistema tecnológico de toda la Administración Pública Estatal. Sabiendo que cada dependencia tiene un nivel distinto de ciberseguridad, se impulsará la elaboración general de lineamientos de desarrollo de software, de infraestructura tecnológica, de gestión de datos y de privacidad, que deberán de tener a consideración la normativa vigente de protección de datos personales y de ciberseguridad, estableciendo los mecanismos mínimos de control de acceso, administración, control y manejo de información, infraestructura tecnológica, desarrollo de software y sistemas que deberán de considerar la ciberseguridad como parte de su planeación, desarrollo, implementación, operación y cierre.

Objetivo 1: Establecer un marco normativo estatal para establecer los estándares mínimos de ciberseguridad para la Administración Pública Estatal.

Establecer un marco normativo estatal que se base en las normas internacionales como ISO, CIS CONTROLS, NIST, entre otras, bajo la dirección de una única autoridad en materia de ciberseguridad que se aplique de manera transversal a los Sujetos Obligados para homogeneizar la normativa en ciberseguridad.

Actividad 1: Desarrollar un modelo de niveles de madurez que permita a los Sujetos Obligados evaluar la situación actual en materia de ciberseguridad, que esté basado en las normativas internacionales y permita la identificación de inversiones prioritarias, orientar planes de mejora y medir el progreso institucional.

Actividad 2: Generar un catálogo estandarizado de controles mínimos por criticidad y nivel de madurez. Los Sujetos Obligados deberán de adoptar el catálogo de controles técnicos y organizacionales obligatorios aplicando por criticidad de los activos digitales y su nivel de madurez, con el fin de orientar el cumplimiento efectivo y garantizar que los recursos se orienten a medidas proporcionales al riesgo que represente su ecosistema de TI.

Actividad 3: Elaborar lineamientos de DevSecOps y desarrollo seguro. Se diseñarán políticas que integren la seguridad desde las primeras fases del ciclo de vida del software con prácticas de DevSecOps, que incluyan revisiones de código y validación de componentes y metodologías de desarrollo seguro.

Actividad 4: Establecer lineamientos de datos y privacidad. Se emitirán lineamientos que garanticen la protección de los datos personales y sensibles bajo un enfoque de ciberseguridad

Actividad 5: Definir procesos de continuidad, respaldos y gestión de excepciones. Cada Sujeto Obligado deberá de contar con un Plan de Continuidad Operativa y con respaldos periódicos que aseguren la recuperación de la información y servicios en caso de incidentes.

Objetivo 2: Fortalecer la coordinación y gobernanza interinstitucional.

La Administración Pública Estatal, requiere una gobernanza efectiva, basada en la colaboración entre los Sujetos Obligados para establecer los mecanismos de coordinación permanentes que aseguren la definición clara de roles y responsabilidades, faciliten la toma de decisiones y fortalezcan la capacidad de respuesta frente a incidentes y amenazas.

Actividad 6: Establecer a la ATD como la autoridad de regulación y gestión de la ciberseguridad con jurisdicción transversal y con capacidad de ejecución.

Actividad 7: Establecer grupos permanentes de coordinación en materia de ciberseguridad con el fin de garantizar el análisis y compartición de información que permita atender temas de ciberseguridad.

Actividad 8: Implementar un modelo que defina roles y responsabilidades, así como designar los enlaces de ciberseguridad en cada Institución del Gobierno Estatal de la Administración Pública Estatal, para garantizar la ejecución y monitoreo de las acciones en materia de ciberseguridad.

Eje 2: Gestión de riesgos y resiliencia operativa

La gestión de riesgos establece un enfoque preventivo en ciberseguridad y un requisito indispensable para asegurar la continuidad de la Administración Pública Estatal en el entorno digital. Este eje estratégico busca implementar un modelo integral y dinámico de gestión de riesgos, capaz de identificar, analizar, priorizar y tratar amenazas de manera uniforme en todas la Administración Pública Estatal.

Objetivo 3: Implementar un modelo de Gestión de Riesgos en la Administración Pública Estatal.

Gestionar los riesgos es clave, para anticipar amenazas y priorizar recursos de manera proporcional al impacto potencial en el ecosistema tecnológico de la Administración Pública Estatal.

Actividad 1: Elaborar y mantener un inventario de activos por criticidad. Cada Sujeto Obligado, deberá identificar, documentar y clasificar sus activos tecnológicos, servicios digitales y procesos críticos.

Actividad 2: Desarrollar e implementar una metodología de gestión de riesgos para la identificación, análisis, evaluación, monitoreo y tratamiento de riesgos, basada en estándares internacionales.

Actividad 3: –Integrar procesos de inteligencia de amenazas y campañas de prevención mediante la implementación de mecanismos de recolección y análisis. Los hallazgos deberán traducirse en campañas de prevención focalizadas, alertas y recomendaciones prácticas que fortalezcan la seguridad de la Administración Pública Estatal.

Actividad 4: Ejecutar pruebas de penetración y ejercicios de restauración en las que cada Sujeto Obligado deberá realizar de forma periódica pruebas técnicas de penetración y ejercicios simulados que validen la eficacia de los planes de respuesta y

recuperación. Estos ejercicios deberán incluir escenarios de restauración de servicios críticos y evaluaciones después de la restauración que aseguren la resiliencia institucional frente a incidentes reales.

Actividad 5: Implementar en cada Sujeto Obligado un plan de Gestión de Recuperación de Riesgos de Ciberseguridad y de Continuidad Operativa.

Actividad 6: Establecer en cada Sujeto Obligado, un registro actualizado de riesgos vinculado a controles técnicos, asegurando su actualización frente a nuevas amenazas, vulnerabilidades críticas o cambios regulatorios.

Objetivo 4: Asegurar la continuidad de servicios públicos esenciales.

La resiliencia institucional depende de la capacidad de mantener en operación los servicios esenciales aún en condiciones adversas, ataques o crisis. Este objetivo busca establecer planes y protocolos que garanticen la recuperación oportuna y segura de los sistemas críticos para asegurar la continuidad de sus funciones estratégicas.

Actividad 1: Elaborar un análisis de impacto, por servicios y que identifique las relaciones críticas del ecosistema tecnológico.

Actividad 2: Establecer modelos de respaldos en cada Sujeto Obligado que permita asegurar la disponibilidad de información frente a incidentes.

Actividad 3: Documentar y mantener actualizado un Plan de Recuperación ante Desastres en cada Sujeto Obligado.

Actividad 4: Elaborar y mantener un Plan de Continuidad Operativa que contempla escenarios técnicos y operativos de contingencia por cada Sujeto Obligado.

Eje 3: Protección de infraestructura crítica y activos tecnológicos

La protección de la Infraestructura crítica constituye un pilar fundamental para la resiliencia digital del Estado. Se busca garantizar que el ecosistema tecnológico estatal opere bajo principios de confiabilidad, disponibilidad e integridad, mediante la adopción de medidas técnicas y organizacionales que fortalezcan su seguridad desde el diseño.

Objetivo 5: Fortalecer la protección de infraestructura y servicios críticos.

Actividad 1: Establecer mecanismos obligatorios de endurecimiento bajo estándares aceptados internacionalmente y configuraciones base comunes para sistemas operativos, bases de datos, entornos en la nube y contenedores.

Actividad 2: Implementar mecanismos de cifrado para la protección de datos, mediante los cuales las dependencias y entidades deberán incorporar medidas de cifrado sólido en tránsito y en reposo.

Actividad 3: Fortalecer la infraestructura de comunicaciones y servicios digitales esenciales, mediante controles de seguridad para redes, centros de datos, servicios en la nube y plataformas críticas, con medidas como redundancia, monitoreo continuo y esquemas de protección perimetral y de aplicación.

Actividad 4: Implementar procesos sistemáticos de gestión de vulnerabilidades y parches, por los cuales las dependencias y entidades deberán adoptar procesos estandarizados de identificación, análisis, priorización y remediación de vulnerabilidades.

Actividad 5: Integrar y mantener un inventario preciso y actualizado de activos tecnológicos críticos, incluyendo su clasificación por nivel de importancia, de manera que se asegure visibilidad y control de los componentes esenciales de la infraestructura de cada entidad.

Actividad 6: Desplegar soluciones de seguridad avanzada en endpoints y servidores (EDR/XDR), que permitan detectar, analizar y responder de manera automatizada a amenazas en los dispositivos y entornos de operación de la Administración Pública Estatal.

Actividad 7: Fortalecer los sistemas de correo electrónico y dominios institucionales mediante la implementación obligatoria de controles como SPF, DKIM, DMARC y mecanismos de protección contra typosquatting, reduciendo así la superficie de ataque vinculada al correo.

Eje 4: Prevención, detección y respuesta a incidentes

La capacidad del Estado para anticipar, identificar y contener amenazas cibernéticas resulta esencial para proteger los servicios públicos y salvaguardar la confianza de la ciudadanía.

Objetivo 6: Consolidar capacidades de monitoreo y respuesta.

Los Sujetos Obligados en conjunto con la ATD deberán adoptar un conjunto de acciones operativas que consoliden un modelo de prevención, detección y respuesta frente a incidentes de ciberseguridad.

Actividad 1: Integrar mecanismos de correlación de eventos y casos de uso compartidos, que permitan consolidar información de seguridad en tiempo real y habilitar una respuesta coordinada y más eficaz frente a incidentes de alto impacto.

Actividad 2: Integrar un comité interinstitucional como instancia técnica de coordinación, encargado de la detección, análisis, y gestión de la respuesta a incidentes que afecten los sistemas y servicios de la Administración Pública Estatal.

Actividad 3: Definir protocolos de intercambio de información, coordinación de

respuesta y escalamiento entre la Agencia de Transformación Digital y los Sujetos Obligados, asegurando trazabilidad y claridad en cada fase del proceso de gestión de incidentes.

Eje 5: Identidad, accesos y Zero Trust

Gestionar y controlar las identidades y accesos al ecosistema tecnológico de la Administración Pública Estatal, constituye uno de los elementos más críticos para proteger la información y los servicios digitales.

Objetivo 7: Garantizar accesos seguros y confiables en toda la Administración Pública Estatal.

Este Objetivo está enfocado en fortalecer la seguridad de accesos y garantizar la protección de la información, por lo cual, los Sujetos Obligados, deberán implementar acciones operacionales orientadas a consolidar un modelo integral de gestión de identidades, MFA y Zero Trust.

Actividad 1: Establecer políticas Integrales de Identidad y Accesos (IAM), que incluyan la definición de lineamientos comunes y la implementación de un flujo estandarizado de gestión del ciclo de vida de las identidades (alta, baja, cambios). Estos procesos deberán integrarse a todo el ecosistema tecnológico de la Administración Pública Estatal para asegurar la trazabilidad y control de las cuentas y privilegios.

Actividad 2: Implementar mecanismos de MFA, priorizando factores resistentes a Phishing. Considerando esto, deberá ser de carácter obligatorio su implementación en trámites, servicios, plataformas, servidores críticos, etc, de manera inicial hasta la implementación total en el ecosistema tecnológico de la Administración Pública Estatal.

Actividad 3: Adoptar el modelo Zero Trust en toda la Administración Pública Estatal, aplicando el principio de mínimo privilegio, segmentación contextual y verificación continua.

Eje 6: Cadena de suministro y terceros confiables

La seguridad de la Administración Pública Estatal, no depende únicamente de sus propias capacidades, sino también de la solidez de los terceros y proveedores que participan en la provisión de productos y servicios tecnológicos, por lo que, los Sujetos Obligados, deberán asegurarse que los consultores, proveedores, integradores de tecnologías, entre otros, cumplan con los estándares internacionales de ciberseguridad y acrediten sus prácticas.

Objetivo 8: Asegurar adquisiciones y servicios con criterios de ciberseguridad.

Los Sujetos Obligados deberán implementar un conjunto de acciones operativas orientadas a asegurar la confiabilidad de sus relaciones con proveedores y terceros, en seguimiento a las disposiciones y recomendaciones que emita a ATD.

Actividad 1: Emitir disposiciones normativas que fortalezcan los procesos de adquisición, arrendamiento y prestación de servicios en tecnologías de información, asegurando que se desarrollen bajo criterios de transparencia, consistencia, integridad y con las mejores prácticas en materia de ciberseguridad.

Actividad 2: Emitir recomendaciones institucionales para la relación con proveedores y distribuidores de productos y servicios de ciberseguridad, que integren técnicos, legales y de integridad.

Actividad 3: Definir y aplicar requisitos contractuales mínimos, cláusulas de seguridad y criterios técnicos, jurídicos y administrativos, que deberán considerarse de manera obligatoria en los procesos de contratación con terceros o partes interesadas en la cadena de suministro

Eje 7: Capacidades técnicas, talento humano y cultura de ciberseguridad

Fortalecer la ciberseguridad en la Administración Pública Estatal, requiere de infraestructura tecnológica robusta y de personas servidoras públicas especializadas en la materia, además de contar con una cultura institucional de corresponsabilidad.

Objetivo 9: Fortalecer el talento especializado y la formación continua.

Actividad 1: Diseñar e implementar talleres, cursos y capacitaciones, enfocados a directivos, personal técnico, jurídico, administrativo y de atención ciudadana.

Actividad 2: Desarrollar un plan de talento en ciberseguridad, orientado a la atracción, retención y capacitación continua de personal especializado.

Actividad 3: Actualizar de manera anual los programas de capacitación, garantizando la atracción y retención de conocimientos.

Objetivo 10: Impulsar una cultura institucional y social de ciberseguridad

Actividad 1: Promover la elaboración y difundir guías de buenas prácticas.

Actividad 2: Promover programas contra phishing y amenazas comunes.

Actividad 3: Establecer un curso obligatorio de ciberseguridad para todas las personas servidoras públicas de la Administración Pública Estatal que proporcione conocimientos básicos y esenciales.

Actividad 4: Elaborar y ejecutar un plan de simulacros de crisis e incidentes, continuidad de operaciones y restauración de servicios.

Actividad 5: Promover campañas de concientización sobre ciberseguridad para fomentar una cultura de ciberseguridad colectiva.

Eje 8: Innovación y mejora continua

La ciberseguridad en la Administración Pública Estatal, requiere de actualización constante en las nuevas técnicas de ataque, en vulnerabilidades encontradas en los sistemas Operativos, plataformas y herramientas utilizadas por los Sujetos Obligados, en métodos de análisis de comportamiento y tráfico web, para generar estrategias adecuadas para los nuevos métodos de infiltración.

Objetivo 11: Fomentar la cooperación y la innovación.

Actividad 1: Colaborar de manera interinstitucional y con iniciativa privada en el desarrollo de tecnologías y herramientas orientadas al análisis de datos para anticipar nuevas amenazas.

Actividad 2: Establecer convenios de cooperación con instituciones académicas, organizaciones de la sociedad civil, organismos internacionales y empresas del sector privado, para potenciar capacidades técnicas y humanas, adoptar tecnologías, coordinar iniciativas y estrategias, compartir buenas prácticas y fortalecer la innovación.

Responsabilidades Institucionales

Agencia de Transformación Digital

A través de su titular, es la autoridad rectora en materia de ciberseguridad en la Administración Pública Estatal y cuenta con las siguientes facultades:

- Emitir disposiciones normativas en materia de ciberseguridad, incluyendo normas, políticas, lineamientos, criterios técnicos y demás instrumentos análogos necesarios para el fortalecimiento de la seguridad de la información y derivados de esta Política;

● Promover la estandarización de procesos, herramientas y controles en materia de ciberseguridad;

● Facilitar la cooperación interinstitucional, nacional e internacional, así como la interoperabilidad normativa en materia de ciberseguridad;

● Establecer mecanismos de coordinación interinstitucional, colaboración y cooperación para asegurar la implementación efectiva de esta Guía y promover la corresponsabilidad entre los Sujetos Obligados.;

● Fomentar la cooperación multisectorial, el desarrollo tecnológico soberano y la adopción de soluciones seguras e interoperables que fortalezcan la resiliencia digital del Estado y la protección de los derechos digitales de la población.

Proporcionar asesoría y capacitación para el cumplimiento de la guía, a los Sujetos Obligados de la Administración Pública Estatal.

● Desarrollar y orientar políticas, lineamientos, normas, guías, metodologías, campañas y cualquier otro tipo de documentación relacionada con la ciberseguridad y seguridad de la información;

● Desarrollar metodologías y herramientas para la gestión de riesgos, cumplimiento normativo, y evaluación de madurez en ciberseguridad;

● Establecer protocolos de respuesta, alerta temprana y coordinación ante incidentes;

● Supervisar, dar seguimiento y acompañamiento al cumplimiento normativo, técnico y organizacional en materia de ciberseguridad;

● Definir, actualizar y mantener una clasificación de niveles de madurez existentes en la Administración Pública Estatal en materia de ciberseguridad considerando estándares internacionales;

● Orientar la priorización de inversiones estratégicas en ciberseguridad

● Desarrollar la propuesta de controles técnicos, físicos y administrativos para la mitigación de riesgos y la mejora continua en materia de Ciberseguridad en la Administración Pública Estatal;

● Cualquier otra que por su naturaleza y las leyes aplicables le confieran.

Sujetos Obligados de la Administración Pública Estatal.

● Adopción y cumplimiento: Implementar esta guía en sus procesos, sistemas y estructuras internas conforme a los lineamientos y normas técnicas que se emitan;

● Planeación institucional: Elaborar y mantener actualizado su Plan Institucional de Ciberseguridad, aprobado por su titular y alineado con esta Guía;

● Gestión de riesgos: Identificar sus activos críticos, evaluar riesgos cibernéticos y aplicar medidas de protección proporcionales;

● Capacitación y cultura: Asegurar la capacitación continua de su personal y promover buenas prácticas en seguridad digital de acuerdo al Lineamiento para la capacitación y sensibilización en ciberseguridad;

● Mejora continua: Establecer mecanismos internos de supervisión, auto-evaluación y remediación;

● Colaboración: Participar en grupos o mesas de trabajo para dar cumplimiento a la Guía de Ciberseguridad, así como en ejercicios, simulacros y redes de cooperación técnica coordinadas por la ATD;

● Inteligencia de amenazas: Recopilar y compartir la información relacionada con incidentes de seguridad para que la ATD esté en posibilidad de analizar, evaluar y determinar las acciones correspondientes de conformidad con la presente guía

- Niveles de madurez: Establecer la hoja de ruta, acciones y controles requeridos para incrementar de manera constante su nivel de madurez en ciberseguridad de acuerdo al Lineamiento establecido en la materia.

- Ejecutar las acciones derivadas de los distintos Lineamientos que acompañarán a esta Guía.

Recomendaciones por tecnologías

Debido al análisis realizado con los reportes anuales generados de Fortinet, Crowdstrike y Rockwell Automation, se detectan los principales objetivos de los ciberdelincuentes detalladas a continuación.

Se emiten recomendaciones para asegurar y proteger el ecosistema tecnológico que presente amenazas o brechas de seguridad, así mismo, se establecen las acciones a implementar de manera inmediata debido a la constante actualización de los mecanismos de ataque. Por esto, las instancias gubernamentales deberán mantenerse actualizadas con las vulnerabilidades encontradas por cada una de las soluciones tecnológicas de su institución con el fin de prevenir posibles ataques que representen riesgos de la integridad de la información, la suplantación de identidad, el secuestro de la infraestructura, la denegación de servicios, entre otros.

Estas recomendaciones, aplican exclusivamente si su institución cuenta con alguna de las tecnologías que se mencionan a continuación.

SIP / VOIP

Servicios de Voz sobre IP expuestos o con controles de autenticación débiles y de exposición continua, permiten tener acceso a los servicios de VoIP. Los ciberdelincuentes pueden llegar a realizar llamadas de fraude con el identificador de llamadas de las instituciones de gobierno conocidas, realizar movimientos laterales (para llegar a otros servidores), realizar llamadas a las mismas extensiones registradas dentro de su conmutador, haciéndose pasar por un alto mando y ordenando realizar transacciones a cuentas externas. Considerando que los conmutadores están conectados a otros sistemas o plataformas (chatbots, contestadores automáticos, etc.) podrían modificar la operatividad y reenviar las llamadas a un número externo para realizar fraudes o extorsiones telefónicas tomando la identidad de la institución de gobierno.

Como defensores, el impacto sería el incremento de probabilidades de puntos de acceso, forzando la exposición SIP como un riesgo operacional constante.

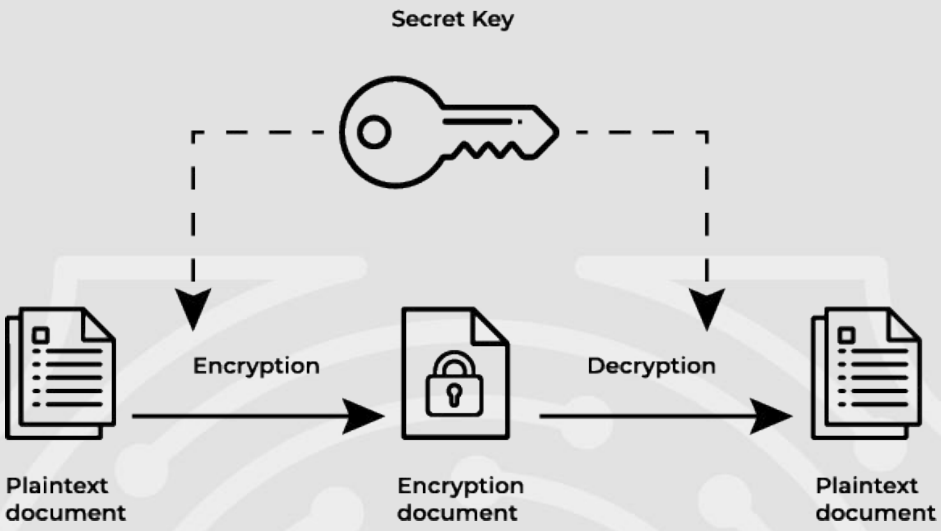
Recomendaciones

Si tu Instancia Gubernamental cuenta con una centralita o conmutador telefónico IP, las recomendaciones mínimas de seguridad a implementar deberán de considerarse como prioridad:

1. Proteger los servicios SIP implementando la encriptación de tráfico, TLS (Transport Layer Security)

TLS utiliza una combinación de criptografía simétrica y asimétrica que proporciona un buen rendimiento y seguridad al momento de transmitir información segura.

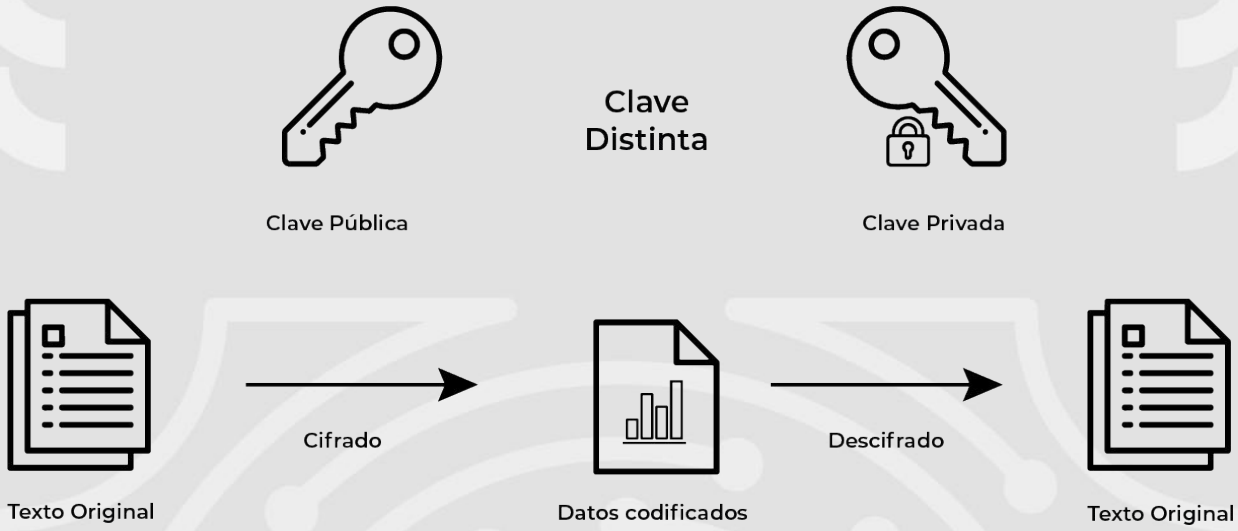
Criptografía Simétrica: Utiliza una única clave compartida para cifrar y descifrar el tráfico que se transmite por internet y en grandes volúmenes de información, lo cual permite que el procesamiento de cifrado y descifrado sea más rápido pero aún con el riesgo de poder ser interceptado el proceso de intercambio de la clave.



(G. J. Simmons/1992)

Encriptación Asimétrica: Utiliza pares de claves o llaves, una pública y una privada, la pública es la conocida, publicada y accesible, pero la privada es única y privada, siendo necesario contar con ambas claves para poder descifrar un mensaje o tráfico en internet, esto permite seguridad la transmisión, además de validar la veracidad del mensaje, ya que la clave privada es única para el cliente, y con esto, auténticas el usuario o usuarios y el origen del mensaje que se está transmitiendo la información.

(G. J. Simmons/"A survey of Information Authentication"/Contemporary Cryptology/ The science of information integrity/ ed. GJ Simmons/IEEE Press, New York/1992)



(Mata Teran, Rolando Manuel,2022)

2. Implementar SRTP (Secure Real-Time Transport Protocol)

Utilizando autenticación y cifrado para minimizar los riesgos de ataques, es flexible por diseño permitiendo utilizar nuevos algoritmos de encriptación, ya que para poder establecer conexión se deberán de autenticarse previamente.

3. Implementar un Session Border Controller (SBC)

Este funcionará como un firewall para el control de acceso de sesiones de VoIP y SIP, que a su vez puede enrutar servicios a distintas oficinas, este se coloca entre el ISP y la red local de la oficina para separar el tráfico entrante de internet como una capa de seguridad adicional al mantener separadas las redes locales de internet

Previene los ataques de denegación de servicios (DDoS), debido a que se encarga de filtrar los paquetes del tráfico de red (específicamente a tu red de voz, denegando los intentos de sesión desconocidos y las sesiones salientes. Adicionalmente, permite la comunicación entre distintos tipos de conmutadores de voz, aunque funcionen en protocolos diferentes manteniendo incluso la estabilidad de la comunicación, aplicando protocolos de Calidad de Servicio (QoS).

Implementar esquemas de conexión cifrada entre los servidores y el cliente, con modelos de autenticación aplicables a cada una de las tecnologías en su institución.

Mata Teran, Rolando Manuel / Criptografía asimétrica / 2022 - https://es.linkedin.com/pulse/criptograf%C3%ADa-asim%C3%A9trica-rolando-manuel-mata-teran

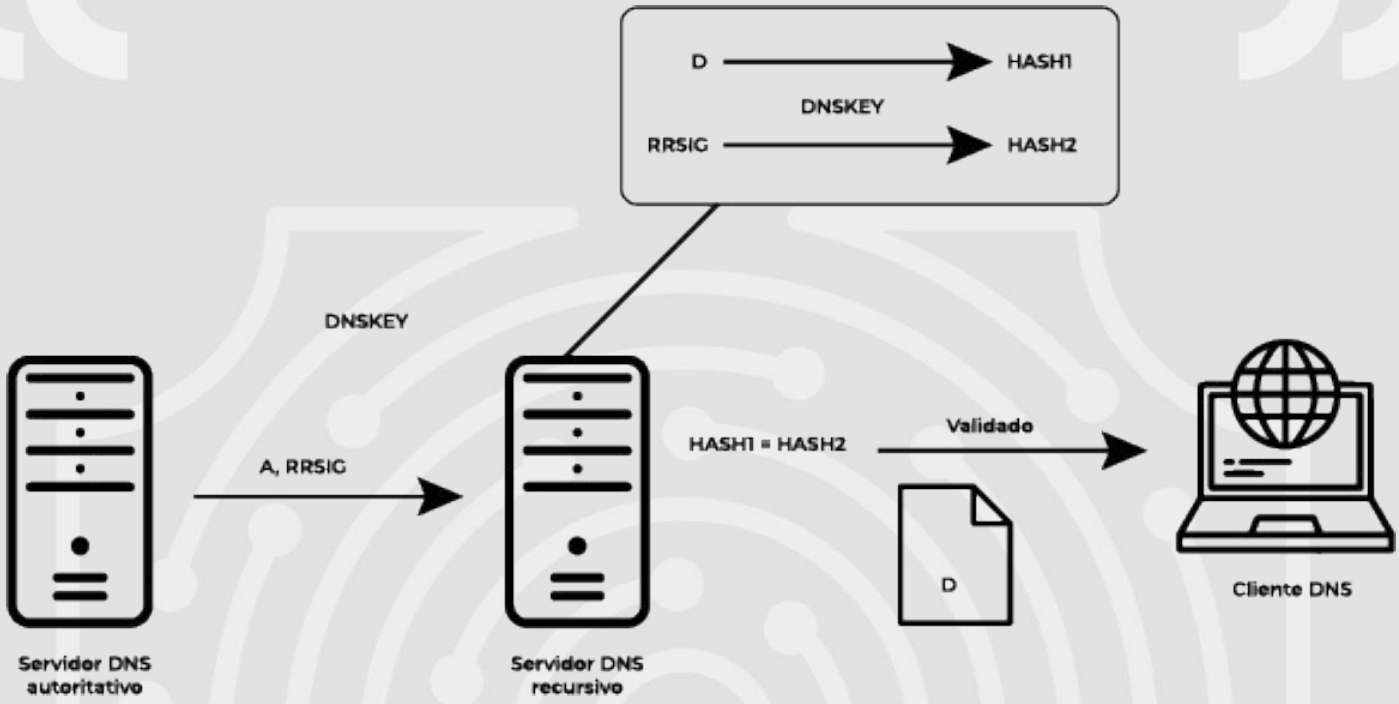
DNS

Servidor de Nombres de Dominio (DNS), es parte de los principales objetivos de los atacantes, debido a que se encarga de redirigir un nombre de dominio a la ip privada del servidor, puede ser utilizado para redirigir el tráfico web a otro sitio, suplantación del sitio, etc.

Es de vital importancia proteger nuestros DNS, aplicando configuraciones que permitan limitar la transferencia de zonas de nombres de dominios, así evitamos que los atacantes puedan obtener la estructura de la red completa.

1. Implementar DNSSEC (Domain Name System Security Extensions)

   Esta función permite autenticar y validar de manera encriptada los nombres de dominio por medio de la firma digital del DNS. Permite garantizar el redireccionamiento a los sitios web legítimos, evitando los sitios fraudulentos y protegiendo de la suplantación de identidad.



(Microsoft Learn 2025)

1. Implementar un sistema o plan de monitoreo constante los DNS de su institución, mantener actualizadas las configuraciones y las tablas de direccionamiento de las zonas del DNS.

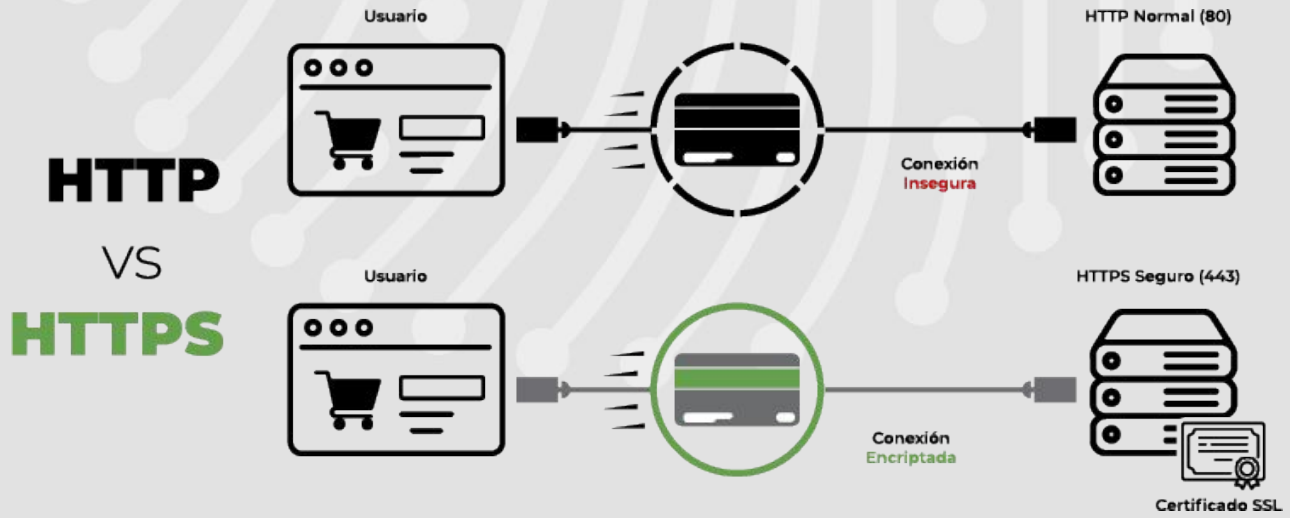
En conclusión, se recomienda agregar como control mínimo la restricción de transferencia de zonas, uso de registros actualizados, monitoreo de cambios no autorizados y revisión periódica de configuraciones DNS.

Microsoft Learn / Introducción a DNSSEC / 2025 / Validación de DNS - https://learn.microsoft.com/es-es/azure/dns/dnssec

Sitios Web de las Instituciones Gubernamentales

Para la administración de sitios web que se encuentran publicados y accesibles a la ciudadanía, es imprescindible la protección de estos sitios para cuidar la imagen institucional estatal, cumplir con la ley de transparencia y acceso a la información pública del Estado de Quintana Roo, brindar información institucional, etc.

Se recomienda mantener el Gestor de Contenido de los sitios con doble factor de autenticación para el inicio de sesión a los servidores. Mantener las carpetas de los servidores con permisos de acceso por usuario ligados a la base de datos del Gestor de contenido. Adicional a esto, agregar el certificado SSL que es la capa de certificación y autenticación del sitio. Dándole seguridad a los sitios web, cifrando los datos enviados entre el servidor y el cliente web y permitiendo al usuario final tener la seguridad de su información. El uso de las tecnologías de la información y comunicación es de relevancia para El Estado, mantenerlas seguras y protegidas aún más. Se emiten estas recomendaciones para las distintas Instituciones de Gobierno que cuentan con alguna de las tecnologías mencionadas en el presente documento con el objetivo de proteger la información de quienes utilizan estos servicios, brindar seguridad a la ciudadanía, disponibilidad de los servicios web y mantener la disponibilidad.



(ADSLZONE, 2025)

ADSLZONE / HTTP VS HTTPS / 2025 -
https://www.adslzone.net/como-se-hace/internet/web-certificado-https/

Conclusión

La ciberseguridad representa actualmente un componente estratégico para la continuidad operativa, la protección de la información y el fortalecimiento de la confianza en los servicios digitales gubernamentales. Ante un entorno tecnológico en constante evolución y con amenazas cada vez más sofisticadas, resulta indispensable que los Sujetos Obligados de la Administración Pública Estatal adopten una visión integral, preventiva y coordinada en materia de seguridad digital.

Actualmente, las capacidades y mecanismos de ciberseguridad dentro de la Administración Pública Estatal se encuentran dispersos, por lo que cada Sujeto Obligado atiende sus necesidades de manera independiente, conforme a sus recursos, capacidades técnicas y criterios institucionales. En este contexto, el presente documento tiene la finalidad de servir como una guía de referencia en materia de ciberseguridad, proporcionando criterios, recomendaciones y requerimientos mínimos que puedan ser consultados y aplicados por las instituciones para fortalecer la protección de sus activos tecnológicos, sistemas de información y servicios digitales.

Adicionalmente, este instrumento busca sentar las bases para la consolidación de un marco común de ciberseguridad dentro de la Administración Pública Estatal, promoviendo la homologación de criterios, la coordinación interinstitucional y el fortalecimiento progresivo de las capacidades técnicas y operativas en cada dependencia y entidad gubernamental.

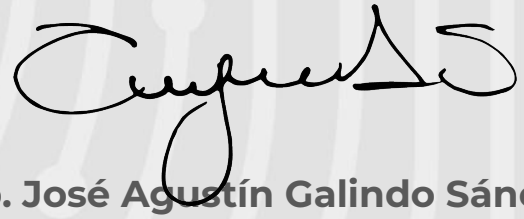
ELABORÓ

Ing. Erick Aldair Tuyub Fuentes.
Jefe de Departamento de Ciberseguridad.

REVISÓ

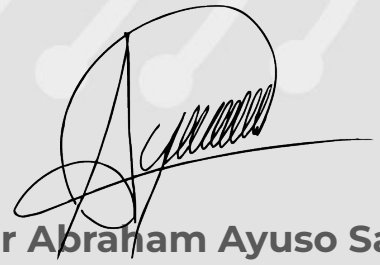
Ing. Dulce Hernández.
Directora de Transformación y Agenda Digital.

VALIDÓ



Mtro. José Agustín Galindo Sánchez.
Coordinador General de Transformación Digital.

AUTORIZÓ



M.E. Javier Abraham Ayuso Sánchez.
Director General de la Agencia de Transformación Digital