SECRETARÍA DE INNOVACIÓN DE LA PRESIDENCIA

POLITICA DE CIBERSEGURIDAD DE EL SALVADOR

INDICE

1. INTRODUCCIÓN

Los avances en la tecnología crean nuevas oportunidades para el desarrollo de las naciones, pero también conlleva riesgos que deben ser abordados de manera adecuada para saber aprovechar los recursos tecnológicos y lograr avanzar en la dinamización de las actividades productivas y de desarrollo de los países.

El Gobierno de El Salvador, a través de la Secretaría de innovación de la Presidencia, ha planificado desarrollar una serie de proyectos que permitirán al país avanzar en materia tecnológica y lograr que la población se beneficie del mundo digital. A través de la agenda digital 2030, se ha planteado una visión de futuro en la cual se contemplan proyectos estratégicos que se interrelacionan y forman un entramado de líneas de acción que en conjunto brindaran el soporte para aprovechar las bondades que las tecnologías de información y comunicaciones ofrecen.

Son muchas las amenazas que están presentes en los entornos de tecnología, pero no son solo amenazas de tipo tecnológico, también las hay en los ámbitos de la gobernabilidad y la gestión de las tecnologías. Según un estudio de las capacidades cibernéticas en la región de Latinoamérica realizado por el BID y la OEA en 2020 (BID, 2020), en El Salvador poco se ha avanzado desde el último estudio realizado en 2016. Este estudio clasifica los países de la región según los avances realizados en materia de ciberseguridad y El Salvador ocupa la posición 96 de ese ranking, por encima de varios países del área centroamericana.

En ese estudio se utiliza un modelo de madurez de la capacidad de ciberseguridad, que entiende la capacidad en cinco dimensiones: (i) política y estrategia; (ii) cultura y sociedad; (iii) educación, capacitación y habilidades; (iv) marcos legales y regulatorios, y (v) estándares, organizaciones y tecnologías. Cada dimensión se desglosa en factores, aspectos e indicadores que permiten evaluar la capacidad de manera progresiva.

En este contexto es importante que el Gobierno de El Salvador desarrolle una política de ciberseguridad y se elaboren las estrategias que fortalezcan la capacidad de ciberseguridad y que proporcionen una guía para que las entidades públicas y/o privadas logren definir y establecer líneas de acción que apoyen el uso de las tecnologías digitales de una manera segura y confiable.

2. OBJETIVO

Establecer las líneas de acción y estratégicas que permitan al Gobierno de El Salvador definir los aspectos relevantes enfocados en la prevención de riesgos cibernéticos, así como la gobernanza que debe existir para obtener éxito en este tema. Es de primordial interés definir los criterios de abordaje para el desarrollo de las capacidades de ciberseguridad enfocadas en el aseguramiento de las infraestructuras críticas, el fortalecimiento de los mecanismos de respuesta ante incidentes y el desarrollo de habilidades técnicas y de gestión, para que las instituciones públicas y privadas a nivel nacional y los ciudadanos mismos puedan tomar conciencia del tema de ciberseguridad y los riesgos del uso de las tecnologías de información, que les permitan adoptar medidas de protección ante las ciberamenazas.

3. ESTRATEGIAS

Para cumplir los objetivos planteados por la política de ciberseguridad se deben establecer las estrategias adecuadas para abordar los temas claves y considerar los aspectos necesarios para lograr cumplir con las metas propuestas por el Gobierno de El Salvador a través de la agenda digital 2030.

A continuación, se presentan las estrategias definidas para lograr establecer los cimientos de un plan nacional de ciberseguridad, las cuales son:

3.1 Creación de la entidad coordinadora de ciberseguridad a nivel nacional

Deberá crearse una entidad que coordine los esfuerzos de ciberseguridad a nivel nacional y que busque los apoyos en todos los sectores interesados, de tal suerte que se logre una colaboración intersectorial en la temática de ciberseguridad, entre el sector público, el sector privado, la academia, las organizaciones no gubernamentales (ONGs) y la sociedad civil.

La entidad coordinadora de ciberseguridad trabajará por establecer las líneas de acción y desarrollar las acciones que sean necesarias para que las estrategias planteadas en esta política se lleven a cabo.

3.2 Concientización en materia de ciberseguridad

Planear y desarrollar campañas de educación en temas de ciberseguridad y riesgos asociados al uso de las TICs en alianza con el sector privado, ONGs y la sociedad civil, con el propósito de crear buenos hábitos de uso de las tecnologías. En las instituciones del sector público se promoverá la capacitación de funcionarios

en temas de ciberseguridad para crear conciencia y con el sector privado se promoverán conversatorios y foros de intercambio de opinión que fomenten el conocimiento en temas de uso seguro de las TICs.

3.3 Reforzar las capacidades en ciberseguridad ante las amenazas

Elaborar un plan de capacitaciones para empleados de gobierno que necesiten reforzar el conocimiento en ciberseguridad a través de la realización de entrenamientos especializados en temas que les ayuden a comprender y fortalecer las defensas ante ataques cibernéticos.

Potenciar la creación de centros de entrenamiento e investigación en la lucha contra ciberamenazas, que permitirán la formación de especialistas que repliquen el conocimiento, realicen pruebas en entornos controlados a manera de investigación y brinden soluciones hechas en casa frente a las necesidades de protección.

Realizar convenios con el sector académico para generar proyectos de investigación y desarrollo de herramientas y soluciones innovadoras contra amenazas emergentes e incidentes cibernéticos.

Promover la adopción del marco de trabajo de ciberseguridad (numeral 5 de este documento) como un estándar, con el fin de establecer controles técnicos y de gestión, que minimicen los riesgos asociados al uso de las TICs

3.4 Reforzar el marco jurídico para la persecución del delito en el ciberespacio y la cibercriminalidad.

Revisión del marco jurídico existente para proponer los ajustes necesarios que permitan responder ante el cometimiento de delitos en el ciberespacio y la ejecución de procedimientos legales que garanticen una adecuada investigación y la realización de juicios justos.

Proponer la creación de una comisión jurídica especializada que verifique la existencia de herramientas procesales adecuadas relacionadas con ciberdelitos y que se encargue de identificar las áreas del sector justicia que deben fortalecer sus conocimientos en materia de ciberseguridad, así como también colaborar para que se capacite a estas áreas identificadas.

Creación de redes de intercambio de información sobre delitos cibernéticos entre actores del sistema judicial para apoyo a los procesos judiciales que contemplen todas las garantías de la cadena de custodia de evidencias y confidencialidad de la información.

3.5 Garantizar la seguridad y resiliencia de activos estratégicos

Desarrollar la normativa que permita la clasificación y protección de los activos estratégicos que brindan servicios esenciales en el territorio nacional, de tal forma que sirva para establecer las medidas de protección de dichos activos, conforme a la evaluación de riesgos de los procesos utilizados en la operación de estos entornos, sin detrimento de los controles establecidos por normativas específicas del sector al que pertenecen.

Crear comisiones con los operadores de las infraestructuras críticas que utilicen activos estratégicos, para la implementación de directrices y lograr una mayor cooperación para la protección de estos activos.

Los operadores de infraestructuras criticas estarán obligados a adoptar un marco de trabajo basado en alguna norma internacional para protección de los activos estratégicos y en la construcción de los mecanismos de resiliencia, como mínimo deberán utilizar el marco de ciberseguridad definido en esta política (numeral 5 de este documento) y la norma ISO/IEC 22301 Gestión de continuidad del negocio.

3.6 Identificación, análisis y gestión del riesgo.

Promover la adopción de un modelo para identificación, análisis y gestión del riesgo que sea adaptable a las necesidades propias de cada organización. Este modelo servirá de apoyo para elaboración de políticas de seguridad institucionales, identificación de planes de acción para implementar el marco de trabajo de ciberseguridad y para la definición de planes de continuidad del negocio.

Fomentar la implementación del marco de trabajo de ciberseguridad que es presentado en este documento, dentro de las instituciones públicas y privadas, de manera cíclica y progresiva, que permita realizar evaluaciones y seguimiento de los controles técnicos establecidos, así como de la madurez de la organización en materia de ciberseguridad, lo cual reducirá los niveles de riesgo.

3.7 Contribuir a la ciberseguridad en el ámbito internacional, promoviendo un ciberespacio abierto, plural, seguro y confiable en apoyo a los intereses nacionales

Potenciar la presencia de El Salvador en foros, conferencias y en la pertenencia a organizaciones regionales e internacionales en materia de ciberseguridad y/o seguridad de la información, así como promover la creación de aquellos medios de participación que posicionen al país ante la comunidad internacional.

Promover el respeto de la Carta de las Naciones Unidades, los tratados internacionales y el Derecho Internacional en lo relacionado a la ciberseguridad y ciberdefensa.

Gestionar la cooperación internacional para apoyar los esfuerzos nacionales en materia de ciberseguridad y ciberdefensa, que permitan dotar de recursos y fortalecer la infraestructura de ciberseguridad del país.

3.8 Fortalecimiento del equipo de respuesta ante incidentes

Garantizar la coordinación, la cooperación y el intercambio de información sobre incidentes de seguridad e inteligencia de ciberamenazas entre el sector público, el sector privado y organismos internacionales, fomentando la prevención y la alerta temprana.

Impulsar y apoyar la creación de equipos de respuesta ante incidentes sectoriales que sean coordinados por el equipo de respuesta ante incidentes nacional (salCERT), con el fin de trabajar coordinadamente y proveer soluciones de protección específicas para cada sector.

Dotar de recursos humanos, técnicos y financieros exclusivos al equipo de respuesta ante incidentes para cumplir con las funciones que debe desempeñar, según lo norman sus estatutos (acuerdo número doscientos dieciocho del Ministerio de Justicia y Seguridad Pública de fecha veintiséis de octubre de dos mil doce).

Fomentar la creación de centros especializados de respuesta ante incidentes de seguridad informática (CSIRT) y Centros de Operaciones de Seguridad (SOC) que se enfoquen en realizar acciones de prevención y respuesta ante incidentes específicos relacionados con el uso de tecnologías digitales, tecnologías emergentes y entornos disruptivos.

4. RESPONSABLE DE CIBERSEGURIDAD

Para poder ser eficaces en el desarrollo de capacidades de ciberseguridad, es importante que se delimiten las responsabilidades y es en ese sentido que la delegación es un tema pertinente y de mucho interés. Para que un plan de acción tenga éxito debe contar con el apoyo pleno de las altas autoridades de cada institución y empoderar al personal delegado para que ejecute los proyectos, de tal suerte que se logre construir una estructura organizativa acorde al entorno de cada institución y que permita lograr con éxito las metas de ciberseguridad.

En cada institución del estado deberá asignarse el rol de coordinador institucional de implementación del plan de ciberseguridad, el cual deberá tener las siguientes funciones: a) comprender plenamente las estrategias de ciberseguridad contempladas en la política de ciberseguridad, b) velar porque se elaboren los

planes de acción para que las estrategias definidas en la política de ciberseguridad logren su cometido, c) coordinar con el responsable de seguridad de la información (RSI) la ejecución de análisis de riesgos y la definición de las líneas de acción a desarrollar para mitigar los riesgos identificados y d) informar al ente coordinador de la función de ciberseguridad en el país de los proyectos considerados en el plan de implementación de la política de ciberseguridad, en concordancia con los riesgos identificados y e) reportar al ente coordinador de la función de ciberseguridad en el país los avances del plan.

Los titulares de cada institución del sector público deberán enviar al ente coordinador de ciberseguridad nacional, la documentación del nombramiento de la persona que ostentará el rol de coordinador institucional de implementación del plan de ciberseguridad.

El comité de seguridad de la información (CSI) de cada institución será el encargado de realizar los análisis de riesgo para definir los planes de mitigación de los riesgos identificados y así formular los proyectos que ayuden a cumplir las metas planeadas en el tema de ciberseguridad. Este comité dependerá directamente del titular que preside la institución y estará formado por al menos el coordinador de implementación del plan de ciberseguridad y por el responsable de seguridad de la información de cada institución. Cada institución podrá incorporar otros miembros al comité, según lo demanden los proyectos a realizar y la dimensión de las líneas de acción a desarrollar.

Las instituciones del sector privado podrán adaptar el modelo de estructura organizativa de acuerdo con el entorno propio y la dependencia del uso de las tecnologías de información para el desempeño de sus funciones. Aquellas instituciones del sector privado que administren infraestructuras críticas y que de ser objeto de ciberataques pudiesen menoscabar el bienestar social y económico de la población en general, deberán implementar un programa de ciberseguridad, según lo dictado en este documento, sin dejar de cumplir normativas ya existentes del sector al que pertenecen.

5. MARCO DE TRABAJO DE LA CIBERSEGURIDAD DE EL SALVADOR (MTCSES)

El marco de trabajo de la ciberseguridad define los lineamientos y buenas prácticas que las Instituciones y organizaciones deben implementar con respecto a la protección de la información, las tecnologías y los servicios digitales que administran, para gestionar los riesgos asociados a la seguridad de la información e infraestructura que la soporta, de conformidad a la línea de acción de ciberseguridad dentro de la agenda digital 2030.

Para la definición del marco de trabajo de la ciberseguridad se ha tomado como referencia el Marco de Ciberseguridad de Uruguay (MCU) (Agesyc, 2020) y el Marco de trabajo de Ciberseguridad definido por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST - National Institute of Standards and Technology, s.f.) para la mejora de la ciberseguridad en infraestructuras críticas. Este marco de trabajo ha sido contextualizado considerando la legislación y normativa vigente para El Salvador y las mejores prácticas internacionales en materia de seguridad de la información tal como la ISO/IEC 27001, COBIT 5 y NIST SP 800-53.

El marco pretende ser una herramienta que permitirá organizar y planificar la estrategia de gestión de riesgos de ciberseguridad de las organizaciones en función de su actividad, tamaño y características específicas y se describe ampliamente en el anexo 3 de este documento.

El marco de trabajo está diseñado para complementar las operaciones de negocio y de ciberseguridad existentes; pudiendo tomarlo como base para la creación de un nuevo programa de ciberseguridad o como herramienta para la mejora de un programa existente.

Tomando como referencia el documento de trabajo “Un abordaje Integral de la Ciberseguridad” (OEA - Organizacion de Estados Americanos, 2019), las organizaciones de El Salvador que requieran mejorar su postura de ciberseguridad deberán estructurar un programa de ciberseguridad utilizando el marco de trabajo definido en esta política y para ello deberán seguir los siguientes pasos:

Paso 1: Priorizar y determinar el alcance. Se deben identificar los objetivos de negocios y las prioridades de alto nivel de la organización. Con esta información se puede determinar el alcance del programa de ciberseguridad: qué línea de negocio o procesos serán abordados.

Paso 2: Orientación. Se identifican los sistemas y activos vinculados al alcance, los requisitos legales o regulatorios, así como el enfoque de riesgo general y de cada uno de los activos dentro del alcance.

Paso 3: Crear un perfil actual. Se realiza una evaluación del programa de ciberseguridad para crear un perfil actual, este indicará qué resultados de categoría y subcategoría del núcleo del marco de trabajo (Framework Core) se están logrando actualmente. Es esencial que esta evaluación incluya Personas (cantidad de

personal, roles de trabajo, habilidades y capacitación para profesionales de seguridad y conocimiento general del usuario), Procesos (estrategia, políticas, procedimientos, manual vs. automatización, canales de comunicación con las partes interesadas, etc.), y Tecnología (capacidades, configuraciones, vulnerabilidades, parches, operaciones y contratos de soporte, etc.).

Paso 4: Realizar una evaluación de riesgos. Se analiza el entorno operativo para discernir la probabilidad de un evento de ciberseguridad y el impacto que el evento podría tener en la organización. Es importante que las organizaciones identifiquen los riesgos emergentes teniendo en cuenta la identificación de vulnerabilidades de los activos y la información de amenazas de ciberseguridad de fuentes internas y externas para obtener una mejor comprensión de la probabilidad y el impacto de los eventos de ciberseguridad. Si bien este paso se enfoca en la identificación de riesgos de ciberseguridad, es importante que este proceso esté alineado a la evaluación de riesgos organizacional, así como a la evaluación de riesgos de negocio para que exista una retroalimentación en las evaluaciones.

Paso 5: Crear un perfil objetivo. Se debe centrar en la evaluación de las categorías y subcategoría del marco de trabajo que describen los resultados deseados de ciberseguridad de la organización, teniendo siempre presente la misión y objetivos del negocio, así como requisitos vinculados a cumplimiento legal o normativo. Las organizaciones también pueden desarrollar sus propias categorías adicionales basados en los requisitos de negocio, así como requisitos de las partes interesadas externas, como son las entidades del sector, los clientes y los socios empresariales; sin olvidar que los requisitos no son únicamente de corte técnico o tecnológico, sino también asociados al personal y capacitación, políticas, procedimientos y demás necesidades administrativas.

Paso 6: Determinar, analizar y priorizar las brechas. Se compara el perfil actual y el perfil objetivo para determinar las brechas. A continuación, hay que crear un plan de acción priorizado para abordar las brechas (que reflejan los impulsores, los costos y los beneficios, y los riesgos de la misión) para lograr los resultados en el perfil objetivo. Luego, la organización determina los recursos necesarios para abordar las brechas, que incluyen los fondos y la fuerza laboral.

Paso 7: Implementar el plan de acción. Se determinan qué acciones tomar para abordar las brechas, si las hay, identificadas en el paso anterior y luego ajusta sus prácticas actuales de ciberseguridad para lograr el perfil objetivo. Es importante que las acciones contemplen todas las aristas de la gobernanza de la ciberseguridad: Personal (contrataciones, capacitación, formación, etc.); Tecnología (soluciones actuales, soluciones comerciales disponibles, nuevos desarrollos, innovación, etc.) y Procesos (políticas, procesos y procedimientos adecuados a la necesidad y realidad de la organización).

Todas las instituciones del gobierno y aquellas entidades que operan infraestructuras críticas estarán obligadas a realizar este procedimiento de 7 pasos, al menos una vez al año y reportar el resultado a la

entidad coordinadora de ciberseguridad, anexando el plan para cubrir las brechas identificadas entre el perfil actual y el perfil objetivo, detallando además los compromisos institucionales para cumplir con el programa de ciberseguridad. En el informe deberá indicarse el nivel de implementación del plan de acuerdo con el modelo de madurez descrito en el anexo 3 de este documento. El informe deberá ser redactado por el coordinador de implementación del plan de ciberseguridad en coordinación con el comité de seguridad de la información (CSI) y será remitido por el representante legal, el funcionario a cargo de la institución o en su defecto por el delegado correspondiente según acuerdos legales en cada institución.

Las instituciones del sector privado que deseen adoptar el marco de trabajo de la ciberseguridad deberán coordinar los esfuerzos con la entidad coordinadora de ciberseguridad nacional.

6. ANEXOS

6.1. ANEXO 1 – Definiciones

Amenazas: Cosa o persona que constituye una posible causa de riesgo o perjuicio para alguien o algo.

Brecha: la separación que existe entre un estado actual de una situación y el estado mejorado de la misma.

Ciberamenazas: Acción, en o a través de un sistema de información que puede resultar en un esfuerzo no autorizado para afectar negativamente la seguridad, confidencialidad, integridad o disponibilidad de un sistema o de la información que transita en éste o se almacena o procesa por este.

Ciberdefensa: Conjunto de acciones de defensa activas, pasivas, proactivas, preventivas y reactivas desarrolladas en el ámbito de las redes, sistemas, equipos, enlaces y personal de los recursos informáticos de la defensa, para asegurar el uso propio del ciberespacio y negarlo al enemigo o a otras inteligencias en oposición.

Ciberdelito: El ciberdelito o delito informático es todo aquel acto ilegal realizado por un delincuente en el espacio digital a través de las redes informáticas y diversos dispositivos electrónicos. Dichos actos ilegales atentan la integridad y confidencialidad de los datos y de los sistemas informáticos, y tienen el objetivo de estafar y robar datos, o simplemente alterar el correcto funcionamiento de los sistemas de información o las infraestructuras que los alojan.

Ciberespacio: Entorno complejo resultante de la interacción de personas, software y servicios en el internet por medio de dispositivos tecnológicos y redes conectadas a este, y que no existe en forma física.

Ciberseguridad: Conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberespacio.

Gobernanza: es el proceso mediante el cual las instituciones públicas manejan los asuntos públicos y gestionan los recursos públicos para promover el estado de derecho y el ejercicio de los derechos

humanos (derechos civiles, políticos, económicos, sociales y culturales). En el ámbito del sector privado se refiere a la forma eficaz y eficiente de administrar las organizaciones.

Incidentes cibernéticos: Acción a través del uso de redes de computadores que tiene como resultado un efecto real o potencialmente adverso en un sistema de información y/o la información que existe en el mismo.

Infraestructuras críticas: Sistemas y redes de información que en ocasión de fallo podrían tener un impacto serio en la salud, seguridad física y operacional, economía y el bienestar de los ciudadanos, o el efectivo funcionamiento del gobierno y la economía del país.

ONGs: Siglas de Organización No Gubernamental.

Resiliencia: En informática se refiere a la habilidad de prepararse para, adaptarse, soportar, y rápidamente recuperarse de interrupciones resultantes de ataques deliberados, amenazas o incidentes accidentales u ocurridos naturalmente.

Riesgo cibernético: se define como cualquier riesgo de pérdida financiera, afectación o daño de la reputación de una organización derivado de algún tipo de falla de sus sistemas tecnológicos de información.

Sector privado: la parte de la economía que no está controlada por el estado, y está dirigida por los individuos y las empresas con fines de lucro.

TICs: Siglas de Tecnologías de Información y Comunicaciones

6.2. ANEXO 2 – Referencias

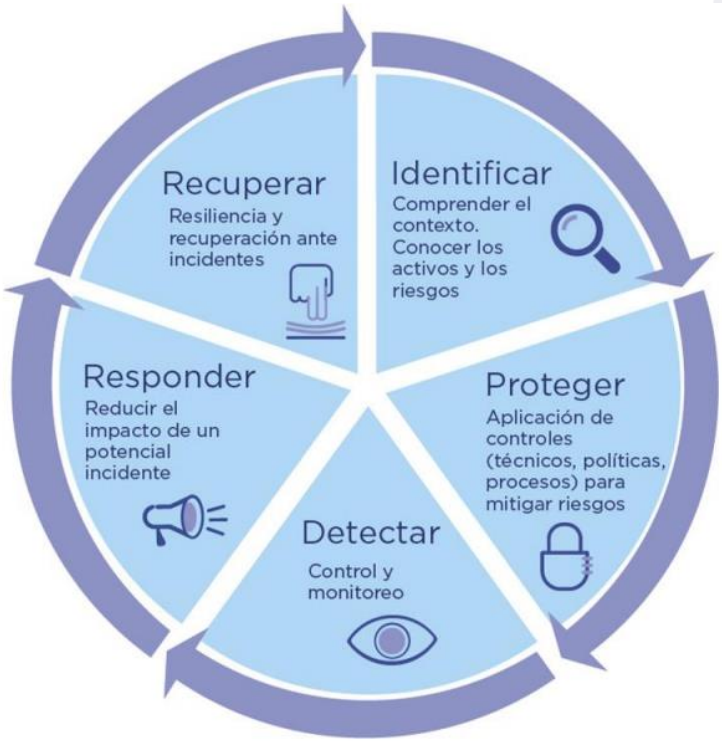
- Reporte de ciberseguridad 2020 – Riesgos, avances y el camino a seguir en America Latina y el Caribe (https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe)
- Carta de las Naciones Unidas (https://www.oas.org/36ag/espanol/doc_referencia/carta_nu.pdf)
- OEA – Marco de trabajo NIST (https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf)
- Estrategia nacional de ciberseguridad de Costa Rica (https://www.micit.go.cr/sites/default/files/estrategia-nacional-de-ciberseguridad-costa-rica-19-10-17.pdf)

- Línea de acción Ciberseguridad en la Agenda Digital de El Salvador (https://www.presidencia.gob.sv/ciberseguridad/)
- Ley especial contra delitos informáticos y conexos (https://www.jurisprudencia.gob.sv/DocumentosBoveda/D/2/2010-2019/2016/02/B6B74.PDF)
- Marco de Ciberseguridad de Uruguay (MCU) – (https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/marco-ciberseguridad)
- Cybersecurity Framework (https://www.nist.gov/cyberframework)
- ISO 27013 responde a una guía de implementación integrada de un Sistema de Gestión de Seguridad de la Información (SGSI), según ISO 27001, y un Sistema de Gestión de Servicios (SGS). (https://www.iso.org/obp/ui/#iso:std:iso-iec:27013:ed-2:v1:en)
- ISO 22301 norma internacional de gestión de continuidad de negocio. (https://www.iso.org/obp/ui/#iso:pub:PUB100442)
- ISO/IEC 27032, nuevo estándar de ciberseguridad (https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en)
- ISO/IEC 27110 Information technology, cybersecurity and privacy protection — Cybersecurity framework development guidelines (https://www.iso.org/obp/ui/#iso:std:iso-iec:ts:27110:ed-1:v1:en)
- ISO 31000 define la Gestión de Riesgos (https://www.iso.org/obp/ui/#iso:pub:PUB100426)
- COBIT 5: Objetivos de Control para las Tecnologías de la Información y Relacionadas (COBIT, en inglés: Control Objectives for Information and related Technology) es una guía de mejores prácticas presentada como framework, dirigida al control y supervisión de tecnología de la información (TI). (https://www.isaca.org/bookstore/cobit-5/wcb5)

6.3. ANEXO 3 – Descripción del Marco de trabajo de ciberseguridad de El Salvador (MTCSES)

El marco de trabajo es una herramienta que permite gestionar la ciberseguridad y provee un enfoque homogéneo para reducir el riesgo vinculado a las amenazas cibernéticas que puedan comprometer la seguridad de la información; está basado en el Marco de Ciberseguridad de Uruguay (Agesyc, 2020) que es una adaptación del marco de ciberseguridad definido por el Instituto nacional de estándares y tecnología (NIST - National Institute of Standards and Technology, s.f.), el cual se compone de tres partes: 1) el núcleo del marco (Core), 2) los niveles de implementación (Tiers) y 3) los perfiles (Profile).

El núcleo del marco de trabajo está constituido por actividades de ciberseguridad, resultados deseados y referencias aplicables que son comunes en todos los sectores de infraestructura críticas, pero que pueden ser aplicadas a cualquier tipo de infraestructura. El núcleo presenta estándares, directrices y prácticas de la industria de una manera que permite la comunicación de las actividades y los resultados de ciberseguridad en toda la organización desde el nivel ejecutivo hasta el nivel de implementación/operaciones. El núcleo consta de cinco funciones simultáneas y continuas: Identificar, Proteger, Detectar, Responder, Recuperar



. Fig.1 Ciclo de vida de la ciberseguridad (Agesyc, 2020)

En conjunto, estas funciones proporcionan una visión estratégica del ciclo de vida de la gestión de riesgos de ciberseguridad en una organización. Dentro de las funciones se identifican categorías y subcategorías que son comparadas con ejemplos de referencias informativas, como estándares, directrices y prácticas existentes para cada subcategoría. Esto permite a las organizaciones alinear su programa de gestión de ciberseguridad con otros estándares de seguridad de la información a nivel internacional en forma práctica y estableciendo objetivos claros.

ESTRUCTURA DEL MARCO DE TRABAJO

Se ha estructurado un cuadro que permite juntar los componentes del marco de trabajo y de esa forma se tenga una herramienta que ayude a visualizar las actividades y los resultados de una manera agrupada. También se incluye en este cuadro la referencia a estándares internacionales (lo cual no pretende ser exhaustivo), así como también los requisitos que son procedimientos básicos que deberá cumplirse en cada subcategoría.

FUNCIÓN	CATEGORÍA	SUB CATEGORÍA	PRIORIDAD POR PERFIL			MADUREZ				REF.	REQUISITOS
			B	E	A	N1	N2	N3	N4		
IDENTIFICAR											
PROTEGER											
DETECTAR											
RESPONDER											
RECUPERAR											

Fig. 2 Estructura del marco de trabajo (Agesyc, 2020)

Las Funciones son el nivel más alto en la estructura del marco para organizar las actividades básicas de ciberseguridad. Las Categorías son la subdivisión de una función en grupos de resultados de

ciberseguridad estrechamente ligados a las necesidades funcionales y actividades particulares. Algunos ejemplos son: “Gestión de activos”, “Evaluación de riesgos”, “Mantenimiento”, y las Subcategorías son los resultados concretos de las actividades técnicas o de gestión, en que se divide una categoría.

Perfiles

Representan las necesidades de ciberseguridad, basadas en los objetivos de la organización, considerando el riesgo percibido y la dependencia existente de las TIC. Cada organización que adopte el marco de trabajo de la ciberseguridad tendrá asignado un perfil sobre el cual trabajar

Se han definido tres perfiles para poder priorizar y establecer el avance en ciberseguridad, los cuales son:

Básico (B): la percepción del riesgo de ciberseguridad es bajo; una falla, disrupción o incidente que pueda afectar los servicios propios, se recuperan utilizando el mejor esfuerzo, no existiendo afectación directa a los objetivos del negocio.

Intermedio (I): la percepción del riesgo de ciberseguridad es moderado, pero existe alta dependencia de las TIC para el cumplimiento de los objetivos del negocio. La disponibilidad de los servicios no soporta más de 48h corridas de interrupción.

Avanzado (A): la percepción del riesgo de ciberseguridad es alto; una falla, incidente o perturbación puede afectar servicios transversales y/o críticos, propios o de terceros. La disponibilidad de los servicios no soporta más de 24h corridas de interrupción.

Prioridad

Las subcategorías del Marco, dentro de un perfil (Básico -B, Intermedio I-, Avanzado -A) tienen asociado un nivel de prioridad de abordaje para su implementación. Las prioridades definidas son:

P1: Subcategoría que forma parte de una línea base de ciberseguridad, de abordaje inmediato y cumplimiento en el corto plazo (hasta 1 año)

P2: Subcategoría que se requiere implementar a mediano plazo (de 1 a 2 años)

P3: Subcategoría que se requiere implementar a largo plazo (de 2 a 3 años)

N/A: cuando no se han identificado requisitos que se ajusten a la subcategoría, en esta versión del marco de trabajo.

Los Niveles de implementación (Tiers)

Los niveles de implementación indican cómo una organización gestiona los riesgos de ciberseguridad, estos describen el grado en que las prácticas de gestión de riesgos de ciberseguridad de una organización son adoptadas. Son similares a los niveles establecidos en un modelo de madurez y describen el grado de rigor en la aplicación de los requisitos de seguridad establecidos en el marco y qué tan bien integradas están las decisiones de riesgo de ciberseguridad en decisiones de riesgo más amplias, así como el grado en que la organización comparte y recibe información de ciberseguridad de fuentes externas.

Se ha definido 5 niveles de madurez, los cuales son descritos a continuación según sus requisitos. Únicamente las categorías que tengan asignado el nivel de prioridad P1 en alguno de los perfiles establecidos serán objeto de evaluación del nivel de implementación, es decir que en cada perfil se analizará el modelo de madurez para las subcategorías que tengan prioridad uno.

Los niveles del modelo de madurez son los siguientes:

Nivel 0: Es el primer nivel del modelo de madurez donde las acciones relacionada con la seguridad de la información y ciberseguridad son casi o totalmente inexistentes. La organización no ha reconocido aún la necesidad de realizar esfuerzos en ciberseguridad. Este nivel no es incluido en el cuadro del modelo de madurez.

Nivel 1: Es el segundo nivel del modelo. Existen algunas iniciativas sobre ciberseguridad, aunque los esfuerzos se realizan en forma aislada. Se realizan implementaciones con enfoques ad-hoc y existe alta dependencia del personal que lleva a cabo las tareas que habitualmente no se encuentran documentadas. Existe una actitud reactiva ante incidentes de seguridad.

Nivel 2: Es el tercer nivel del modelo de madurez. Se han establecido ciertos lineamientos o pautas para la ejecución de las tareas, pero aún existe dependencia del conocimiento individual. Se ha avanzado en el desarrollo de los procesos y existe cierta documentación para realizar las tareas.

Nivel 3: Es el cuarto nivel del modelo de madurez y se caracteriza por la Formalización y documentación de políticas y procedimientos, así como implementaciones de alta complejidad y/o automatizaciones que centralizan y permiten iniciativas de gobernanza. Las políticas y procedimientos son difundidos, facilitan la

gestión y posibilitan establecer controles y métricas. Los esfuerzos en ciberseguridad se enfocan en los procesos, las personas y la tecnología.

Nivel 4: Es el último nivel del modelo de madurez. El responsable de la Seguridad de la Información (RSI) tiene un rol clave en el control y mejora del Sistema de Gestión de Seguridad de la Información (SGSI) realizando o coordinando actividades de control interno para verificar cumplimientos y desvíos. Se desarrollan las lecciones aprendidas que, junto con los controles determinan las acciones para la mejora continua. Las partes interesadas son informadas periódicamente, lo permite alinear los esfuerzos, estrategias y tecnologías de ciberseguridad con los objetivos y estrategias de la organización.

El marco de trabajo de ciberseguridad completo con todas las funciones, categorías, subcategorías, referencias y requisitos, esta descrito en el documento “Modelo del Marco de trabajo de Ciberseguridad de El Salvador”. Una descripción detallada de los requisitos de cada subcategoría se describe en la “Guía de implementación del Marco de trabajo de Ciberseguridad de El Salvador”