UNIVERSIDAD DE LAS CIENCIAS INFORMÁTICAS

FACULTAD 2

Regulación del MINCOM para la gestión segura de los bienes informáticos

Seminario de Gestión de la Ciberseguridad

Integrantes:

Erick Carlos Miralles Sosa:erickcms@estudiantes.uci.cu

Keylan Valdés García:keylanvg@estudiantes.uci.cu

Sheila Hernández Falcón:sheilahf@estudiantes.uci.cu

Sabrina D'Lory Ramos Barreto:sabrinadlrb@estudiantes.uci.cu

Marcos Daniel Artiles Delgado:marcosdad@estudiantes.uci.cu

Introducción

Con el transcurso del avance tecnológico surgen a la vez diversas vulnerabilidades en el empleo de las telecomunicaciones, debido a esto es necesario establecer un conjunto de normas a cumplir para evitar posibles ataques.De esta manera en nuestro país en el 2019 el MINCOM aprueba la Resolución 128/2019 el cual es el documento normativo emitido por el Ministerio de Comunicaciones de Cuba,el cual tiene como objetivo regular las buenas prácticas para la utilización de las telecomunicaciones.

En este análisis, nos adentraremos en los respectivos apartados de la resolución, examinando en detalle cada uno de ellos y analizando su contenido. A través de este estudio, pretenderemos comprender las definiciones y regulaciones establecidas en cada apartado, así como su aplicación en el contexto de las telecomunicaciones cubanas. Enfocándonos fundamentalmente en el capítulo de bienes informáticos, donde estaremos analizando cuales son las principales instituciones de nuestro país que implementan estas series de normativas y como surgieron las buenas prácticas que aplican a las demás instituciones.

Desarrollo

En todas las organizaciones deben realizarse acciones preventivas para evitar riesgos derivados de un mal uso de activos informáticos.Los bienes informáticos son parte fundamental de estos activos por lo que el MINCOM en su Resolución 128/2019 les dedica una sección de buenas prácticas sobre estos.

En esta sección esta resolución del MINCOM exponen varios artículos, donde tienen gran peso el 7, el cual se encarga de establecer los requerimientos de seguridad necesarios en la gestión de bienes informáticos de cada institución, con la correspondiente evaluación de riesgos,vulnerabilidades,la imposición de sanciones ante violaciones de los

sistema de seguridad y en la elaboración de procedimiento ante la recuperación de ataques informáticos.

Fundamentalmente para cumplir con este artículo es necesario saber que los bienes informáticos de la entidad tienen diferentes valores y por lógica son sometidos a diferentes riesgos,por lo que lógicamanete surge la necesidad de llevar a cabo análisis de riesgos para la valoración de la protección de los sistemas y una correcta gestión para evitar esas vulnerabilidades (segurmatica.cu,septiembre 2022)

La pertinencia de este artículo se ve a diario en gran parte las instituciones gubernamentales y no gubernamentales pues es esencial llevarla a la práctica pues protege de cualquier intento de aprovechamiento de vulnerabilidades por parte de algún intruso.

Sabiendo de la importancia del cumplimiento de estas regulaciones por parte de toda la sociedad,la empresa Segurmática llevó a cabo una serie de encuestas en distintas empresas que dieron como resultado la existencia de dudas y necesidad de información sobre el tema y llevan a cabo cursos de adiestramiento online llamados “Análisis y Gestión de Riesgos” donde cualquier persona puede participar pero específicamente va dedicado al personal de la seguridad informáticas de cualquier institución. Acá brindan información sobre los estándares internacionales recomendados a emplear como los estándares internacionales como las normas ISO/IEC 27001 y 27005, además explican sobre las propias normas cubanas sobre todo la propia Resolución del MINCOM 128/2019.

Otra empresa que la lucha por el estricto cumplimiento de este artículo no es más que la propia Empresa de Telecomunicaciones de Cuba(ETECSA), la

cual establece un planteamiento de seguridad más específico que la llevada a cabo por el MINCOM.

Específicamente sobre los requerimientos de protección de los bienes informáticos reflejan prácticamente el mismo consejo de Segurmática que cada entidad es responsable de llevar a cabo su sistema de seguridad,todo con el objetivo de poder minimizar los riesgos sobre los sistemas informáticos y garantizar la continuidad sobre los sistemas informáticos con las medidas necesarias para la prevención de vulnerabilidades.Otras empresas que sugieren sobre estas medidas de seguridad son BioCubaFarma,ETi, entre otras.

Después del anterior análisis podemos concluir que el Artículo 7, como refleja la propia Segurmática necesitaría ser más explícito y aclarativo para que pueda ser entendido de manera más fácil tanto por especialistas , como cualquier individuo, además como aclara ETECSA sería necesario que el artículo fuera más explícito a la hora de aclarar sobre las posibles sanciones ante violaciones del Sistema de Seguridad y la elaboración de los procedimientos de recuperación ante incidentes de seguridad y en sus pruebas posteriores.En cuanto a la eliminación de una parte de este artículo de momento no hay recomendaciones oficiales, solo se recomiendan modficaciones,algunas de las cuales fueron mencionadas y la necesidad de agregar otros elementos al artículo.

Un artículo muy similar al desarrollado anteriormente es el Artículo 6, en cambio otros artículos que necesitarían también un análisis conjunto por su similitud serían los 9,10 y 11 los cuales en resumen hablen sobre la necesidad de que los bienes informáticos estén correctamente custodiados por las personas encargadas de su cuidado, siendo esta responsable de su protección y no divulgación, pero sin obviar que el jefe de la entidad tiene que brindar la tecnología necesaria para garantizar los procedimientos que se requieran, todo esto con el fin de garantizar la autorización y el control sobre la utilización y movimiento de los bienes informáticos.En cambio también se

informa el de uso de empleo y responsabilidad de los bienes informáticos como evitar la no conservación de datos sensibles ni importantes ,la comunicación en caso de la posible pérdida de cualquier bien informática, medida que debe exigir que la cumpla todo empleado.

En las diferentes instituciones se llevan a la prática lo regulado en estos artículos, además también ETECSA emplea como se mencionó anteriormente su propio planteamiento de seguridad,para el correcto cumplimiento de lo acordado en estos artículos.

En el planteamiento de seguridad de ETECSA en su ARTÍCULO 9 se aborda la responsabilidad de los jefes de las instituciones a las diferentes instancias en los órganos, organismos y entidades , donde se les exige identificar la necesidad y cuales son los requerimientos de seguridad necesarios que debe presentar los bienes informáticos bajo su responsabilidad, así como participar en la confección del diseño y elaboración de los sistemas de seguridad.También abordando la necesidad de la instrucción de todo el personal sobre la seguridad de la comunicación y en que se lleven a cabo las correctas sanciones al personal que viole estas normas,también exigiendo la participación en la elaboración de planes de recuperación de los bienes perdidos o dañados.

Este mismo sistema de seguridad también para la correcta pertinencia de estos artículos de la Resolución 128/2019 se especifica sobre el rol que tiene el encargado o los encargados de las actividades informáticas de las entidades,siendo estas bastantes similares a las que tiene el jefe de las instituciones correspondientes.

Alguna de las obligaciones que se especifican son la obligatoriedad de la participación tanto en el diseño como en la implementación de la Seguridad, la imposición y logran que perduren los controles para la protección por el sistema de seguridad informática que se emplea en la institución garantizando en todo momento la disponibilidad de estos.También en su trabajo se incluye

el asesoramiento en las distintas instancias, además como mismo el jefe debe forma de los establecimientos de controles de seguridad y en la participación de procedimiento para la recuperación de bienes en caso de incidentes, estos también forma parte y como último hablan de la necesidad de la comunicación de las medidas que establezcan sobre las regulaciones establecidas.

Por lo tanto en resumen al menos en nuestro criterio según lo visto y analizado se deben llevar a cabo la eliminación o modificación del Artículo 9 pues puede dar lugar confusión el siguiente fragmento:"Los bienes informáticos están bajo la custodia documentada legalmente de la persona designada".Pues una persona incluso el jefe de una institución que lea solo ese artículo puede pensar que la responsabilidad solo es del que manipule el bien y que el jefe y encargado quedan impunes de la seguridad de este.

También se recomienda la adición de lo regido por la administración de seguridad de ETECSA, la aclaración de las responsabilidades que tiene tanto el jefe como los encargados de la seguridad informática de las empresas, además se debe mencionar que también es necesaria no descarta la posible pérdida de bienes informáticos por "falsos clientes" que se encarga al robo de datos o por errores de verdaderos clientes.

Conclusiones

Es importante destacar que la falta de adiciones de fragmentos puede deberse a diversas razones, como la reciente emisión de la resolución, la ausencia de discusión y debate público en torno a ella, o simplemente a que no se han identificado áreas específicas de mejora o modificación.

Sin embargo, se resalta la importancia de continuar investigando y evaluando la resolución en función de posibles cambios y actualizaciones en el futuro. Esto podría involucrar consultas a expertos del sector, consulta pública y diálogo abierto con los actores involucrados, y análisis de experiencias internacionales en la regulación de las telecomunicaciones.

Referencias Bibliográficas

- GOC-2019-O39<<GACETA OFICIAL DE LA REPÚBLICA DE CUBA>>cubadebate.cu
- Laritza González Miranda<<Herramienta para auditorías de seguridad informática>>portalamerica.org, 21 de septiembre de 2022
- Perdomo Di-Lella José Luis<<REGLAMENTO DE SEGURIDAD DE LAS TIC>>,segurmatica.cu,24 de junio de 2019
- segurmatica.cu<<Análisis y Gestión de Riesgos>>Segurmática, 20 de septiembre de 2022
- ucm.gtm.sld.cu<<Herramienta para auditorías de seguridad informática>>Universidad de Guantánamo,2023