PLAN DE CIBERSEGURIDAD PARA EDUCACIÓN BÁSICA ECUATORIANA CONTRA EL CIBERDELITO POR COVID-19

CYBERSECURITY PLAN FOR ECUADORIAN BASIC EDUCATION AGAINST CYBERCRIMEBY COVID-19

Andrade Vintimilla Julio Fernando [1]

[1] Instituto Superior Tecnológico con Condición de Universitario "Compou Sur". Ecuador. julioan652@gmail.com, https://orcid.org/0000-0001-9928-846X

RESUMEN

Debido al ataque del Coronavirus Disease se genera una situación particular que obligó a renovar la forma de trabajar a prácticamente todas las instituciones públicas y privadas del mundo, sin que las instituciones educativas hayan sido la excepción. Se popularizó el teletrabajo y la educación en línea. La condición *sine qua non* para que ocurra el ciber ataque fue que la víctima disponga de una conexión a Internet. Esta se constituye en una circunstancia suficiente y necesaria para que aparezca en el escenario el ciber delito en todas sus formas, teniendo en los estudiantes, su presa fácil por el desconocimiento sobre medidasde prevención para frenar o al menos mitigar este tipo de afectación. Frente a esto, las autoridades de Educación Media del Ecuador deciden emitir una "Normativa para regular la implementación de la educación abierta en el Sistema Nacional de Educación", la cual exige la presentación e implementación del "Plan de Ciberseguridad en Educación Abierta". Este artículo tiene como objetivo proponer un esquema que apoye a la elaboración de un plan de ciberseguridad con miras a frenar los ciberataques provocados por la educación en línea, incluyendo en el mencionado plan, las partes que lo componen, la forma cómo desarrollarlo, quién lo debe revisar y aprobar, cómo implementarlo y cómo retroalimentarlo para que se convierta en un plan dinámico, actualizado que responda a lo esperado por la institución y por los entes de control del Ecuador.

PALABRAS CLAVES: Plan de ciberseguridad, Delito informático, COVID-19.

ABSTRACT

Due to the attack of the Coronavirus Disease, a particular situation arose that forced practically all public and private institutions in the world to renew the way of working, and educational institutions were no exception. Teleworking and online education became popular. The *sine qua non* condition for the cybercrime to occur was that the victim must have an Internet connection. This is a sufficient and necessary circumstance for cybercrime to appear on the scene in all its forms, having in students, their easy prey due to the lack of knowledge about prevention measures to curb or at least mitigate this type of affectation. Faced with this, theauthorities of Secondary Education in Ecuador decided to issue a "Regulation to regulate the implementation of open education in the National Education System", which requires the presentation and implementation of the "Cybersecurity Plan in Open Education". This article aims to propose a scheme to support the developmentof a cybersecurity plan to curb cyber-attacks caused by online education, including the parts that make up theplan, how to develop it, who should review and approve it, how to implement it and how to provide feedbackso that it becomes a dynamic, updated plan that responds to the expectations of the institution and the control entities of Ecuador.

KEYWORDS: Cybersecurity plan, Computer crime, COVID-19.

INTERNACIONAL

A inicios del 2020 el mundo se sorprendió por la aparición repentina de un acontecimiento propiode las películas de ciencia ficción: el ataque del Coronavirus Disease de diciembre 2019 (COVID-19). Para Deloitte (2020), la situación excepcional generada por la mencionada pandemia, está teniendo importantes implicaciones en el ámbito sanitario, económicoy social.

Esta situación obligó a renovar la forma detrabajar, se popularizó el llamado "Teletrabajo" yla educación online. Según EDUCAWEB (2020), expertos del ámbito educativo señalan que paraobtener provecho a la educación en línea hay que estar convencidos de que funciona y ser conscientes de que requiere un esfuerzo extra. Mencionan nueve recomendaciones para sacarle partido a ella:

1. Confiar en la educación en línea.
2. Contar con los recursos informáticos y de conectividad necesarios.
3. Tener competencias digitales para elestudio o disposición para adquirirlas.
4. Ser consciente de que estudiar en línearequiere un esfuerzo añadido.
5. Elegir el mejor lugar para estudiar.
6. Organizarse bien: planificar, marcar objetivos diarios y darles seguimiento.
7. Planificar también los descansos.
8. Interactuar con los docentes y los compañeros.
9. No olvidar gestionar las emociones y compartirlas.

Las sugerencias uno (1) dos (2) y tres (3), tienen relación con la temática del presente documento, por su concordancia con las tecnologías de información y comunicación. Por otro lado, la pandemia del COVID-19 tiene a más del 90 % de los estudiantes del mundo de 188 países confinados en sus casas y sin clases presenciales, según los últimos datos de la UNESCO al 7 de abril de 2020. Poco se habla, sin embargo, del cibercrimen y de cómo esta actividad fraudulenta está incrementando su número de delitos amparándose en la emergencia sanitaria. Junto con esta modalidad de trabajo y educación, lastimosamente se populariza también el concepto de cibercrimen, el cualexiste prácticamente desde que se empieza a usar el Internet. Pero ¿Qué es el cibercrimen? Kaspersky (s.f.) define al cibercrimen como unaactividad delictiva dirigida a un ordenador, una red informática o un dispositivo en red.

Ahora bien, el Internet es la autopista suficiente y necesaria para que exista la ciber delincuencia.Si las computadoras, laptops, tablets, teléfonosinteligentes, o demás dispositivos no están conectados al Internet, no hay peligro de ser afectado por los ciber atacantes, pues no tendrán cómo acceder a la información. Pero, ¿quién no usa Internet en la actualidad? Por tanto, todos estamos expuestos de una u otra manera a este tipo de afectación.

Pero, ¿Quiénes son los que sacan provecho dela situación mencianada? La mayor parte del cibercrimen, pero no todo, está cometido por cibercriminales o hackers que desean ganardinero. El cibercrimen lo cometen personas u organizaciones. Algunos cibercriminales están organizados, utilizan técnicas avanzadas y cuentan con grandes habilidades técnicas. Otros son hackers novatos. En raras ocasiones,el cibercrimen tiene como objetivo dañar los ordenadores por motivos distintos de la obtención de dinero. Estos pueden ser políticos o personales.

En ese mismo orden de ideas, en el pasado se podía suponer que la información que operan los centros de capacitación y formación de acuerdoa su línea de negocio, no sería atractiva para los ciber atacantes. Pero de acuerdo con el reporte"Internet Security Threat Report" de Symantec, el sector educativo se encuentra en el tercer puesto de reporte de brechas de seguridad y en noveno lugar de entidades expuestas a brechas, lo cual desdice la suposición antes mencionada.

Tanto es así que, el ciber crimen en el sectorde la educación, es más frecuente de lo que sepiensa. Según Ona Systems (2018), la falta de control y deficiencia de una política de seguridadinformática en las instituciones educativas son un atractivo para los cibercriminales. Los centros educativos mantienen depósitos de datos sensibles, incluyendo información financiera y estadística.

Segùn Esguerra (2020), nuestros adolescentesde hoy forman parte de la Generación Z, son jóvenes que han nacido y crecido en la era de las nuevas tecnologías, no conciben un mundodesconectado, sin acceso a Internet o a redes sociales. Desde pequeños se han manejado con computadoras, tabletas y smartphones, son complementos de uso diario en sus vidas. Junto a esto, los datos también nos indican que el cibercrimen cada vez atrae y se vincula más con población adolescente. En una encuesta reciente realizada por una compañía de seguridad en línea, aproximadamente 1 de cada6 adolescentes en los EE. UU. y 1 de cada 4 adolescentes en el Reino Unido informaron que habían intentado alguna forma de "piratería" deInternet.

Pero debido a la falta de personal capacitado eneste tipo de instituciones, la falta de inversión y la no adecuada implementación de soluciones de seguridad, la información académica es bastante atractiva para alguien que quisiera atacar información sensible de los docentes, estudiantes, administrativos y padres de familiacomo es el caso de notas, números de cédula, tipos de pago y/o financiación, direcciones de domicilio, nombres de representantes, profesión,lugar

de trabajo, y, en general información sensible que puede servir para dolo, plagio,fraude, secuestro de información, entre otras formas de afectación que pueden ser llevadasa cabo por los ciber delincuentes.

Por citar un ejemplo. El cibercrimen tiene un impacto notable en las instituciones españolas, incluidas las de educación. Según datos del Ministerio del Interior, en España se registraron 110.613 ciberataques durante 2018, siendo la Comunidad de Madrid, Andalucía y la Comunidad Valenciana las regiones donde estos incidentes fueron más recurrentes. En 2019, hasta 174 municipios españoles fueron afectados por campañas con el conocido virus ramsonware. Todo ello, tiene unas graves consecuencias para el desarrollo de las actividades académicas.

El COVID-19 ha encaminado a empresas, instituciones de todo tipo, incluidas las educativas, y Administraciones Públicas a habilitar el teletrabajo para sus empleados y la educación online para la comunidad formativa. Esto se ha producido de manera repentina por lo que, sin duda, obliga a reforzar la ciberseguridad.

En este escenario, si no se toman medidas, se puede llegar a perder el control del entorno en elque trabajan los docentes y estudiantes, como la seguridad en el acceso a las redes wi-fi o,los dispositivos electrónicos que están usando donde no hay limitaciones para descargar cualquier aplicación, igual supone un riesgo muy alto.

Entonces, ¿Qué hacer? Ciertos autores como Avellán Zambrano & Zambrano Bravo (2019), sugieren utilizar estándares para hacer frenteal ciber crimen, como la norma ISO 27032, que permite determinar los riesgos, amenazas y vulnerabilidades de los sistemas distribuidos.

Se debe identificar y evaluar el nivel de riesgosen cada dominio de seguridad (Información, Redes, Aplicación), para poder plantear otras medidas o soluciones sugeridas de mejora ya sea a corto, mediano o largo plazo en aspectos de integridad, disponibilidad y confiabilidad de la información.

Para ello, las instituciones deben poseer en sus departamentos de Tecnologías de Información y Comunicación personal capacitado enSeguridad de Información, quienes deben elaborar planes o al menos un plan básico de ciberseguridad para la institución educativa, la cual debe ser aprobada, apoyada administrativa y financieramente por las máximas autoridades,conocida, entendida y aplicada por todas las personas que forman parte de la institución, para frenar los ciber ataques externos.

Pero, ¿Qué es un plan básico de ciberseguridad? Según el portal Significados (2017), un plande acción es una herramienta de planificación empleada para la gestión y control de tareaso proyectos. Como tal, funciona como una hoja de ruta que establece la manera en que se organizará, orientará e implementaráel conjunto de tareas necesarias para la consecución de objetivos y metas. La finalidad del plan de acción, a partir de un marco de correcta planificación, es optimizar la gestión de proyectos, economizando tiempo y esfuerzo, y mejorando el rendimiento, para la consecución de los objetivos planteados.

Ahora bien, el 24 de julio de 2020 se expideen el Ecuador la "Normativa para regular la implementación de la educación abierta en el Sistema Nacional de Educación", por parte de la Sra. María Monserrat Creamer Guillén, Ministra de Educación.

En el Artículo 7 del mencionado documento se hace referencia a los requisitos para la creación y autorización de funcionamiento de instituciones educativas para ofertar Educación Abierta. Se menciona que, a másde los requisitos establecidos en el artículo 92 del Reglamento General a la Ley Orgánica de Educación Intercultural, para la obtención de la autorización de creación y funcionamiento de las instituciones educativas, debido a las particularidades que tiene la Educación Abierta, se deberá presentar adicionalmente nueve requisitos que son comunes para todas las instituciones educativas, siendo el octavo un "Plan de Ciberseguridad en Educación Abierta", sin precisar información adicional alguna, lo cual se constituye en un hito para este nivelde educación ecuatoriano, por su carácter de novedad.

En vista que la normativa mencionada está en plena vigencia y es de obligatorio cumplimientopara las instituciones educativas públicas, para las fiscomisionales, y para las particulares, incluyendo aquellas que cuentan con su respectiva autorización de funcionamiento, aquellas que cuentan con su autorización de funcionamiento en estado de emergencia, oaquellas que son nuevas pero cuentan con autorización para brindar Educación Abierta, se hace necesario conocer la estrategia para frenar la ciberdelincuencia en los centros de enseñanzaa través de un "Plan de Ciberseguridad en Educación Abierta", lo cual responderá a la necesidad actual de las instituciones que ofertan educación abierta en el nivel general básico para la ciudad de Quito.

Es por esta razón que, en el desarrollo de este artículo, se propone entender el objetivo de un plan de ciberseguridad, cuáles son las partes que lo componen, cómo desarrollarlo, quién lo debe revisar y aprobar, cómo implementarlo y cómo retroalimentarlo para que se convierta en un plan dinámico, actualizado que responda a loesperado por la institución y los entes de controldel Ecuador.

Con esto en mente, se realizó una investigación documental sobre planes de ciberseguridad, pero no se encontró la estructura de un plan con las características requeridas, es decir, que se acople a

instituciones de educación superiory menos aún, de Ecuador.

Pero sí, un grupo de información nacional e internacional que necesitaba ser conectada para ir dando formaa un plan que sea aplicable a quienes estaban siendo partícipes de la educación abierta. Se recopiló información sobre algunas estructuras de planes, por un lado, y las actividades que sedeben controlar como parte de la ciberseguridad en una institución educativa, por otro, para sobre esa fuente de información, ajustarla ala elaboración de un plan de ciberseguridadque se pueda aplicar a la educación abierta ecuatoriana.

Por lo expuesto, se debe entender muy bien qué es y qué partes constituyen un plan;de modo idéntico se debe conceptualizarlo que es el cibercrimen, los ciberataques yla ciberseguridad. Posteriormente, se debe explicar qué es la educación abierta y por qué repentinamente se generalizó.

En concordancia con lo expuesto, se debe relacionar y unir toda la información indicada para dar formaal plan de ciberseguridad para educación abierta. Finalmente, se debe ajustar el plan para que pueda ser usado por las instituciones de educación general de la ciudad de Quito, a manera de plan piloto.

Cabe mencionar que los materiales usados para diseñar el plan lo constituyeron los documentos obtenidos a través de la investigación documental. La normativa de obligatorio cumplimiento también se constituyó en un elemento fundamental, que justificó la elaboración del presente artículo, pues se requería de una estructura que sirva de guía para elaborar un plan de ciberseguridad.

METODOLOGÍA

Materiales y métodos

La desalineación entre la seguridad y el proceso central del negocio tiene un efecto corrosivoen cualquier esfuerzo de seguridad. Y amedida que las instituciones se transforman enservicios digitales, se enfrentan a un aumento de riesgos y de regulación para controlarlos en áreas relacionadas con las Tecnologías de Información.

Alinear la seguridad con los líderes institucionales y los procesos es exponencialmente más importante por la situación actual de la educación online debido ala pandemia del Covid 19.

Por tanto, es necesario desarrollar un plan racional de trabajo para controlar los riesgos relacionados con la seguridad de la informaciónen la búsqueda de la alineación entre la ciberseguridad y los fines de la institución educativa.

El plan desarrolla una metodología que incluye los siguientes pasos:

1. Definir las áreas de enfoque prioritarias y las partes involucradas.
2. Realizar una evaluación del estado ac-tual de la Seguridad de la información.
3. Definir objetivos de mejora (dentro de las áreas de enfoque prioritarias).
4. Identificar métricas.
5. Realizar seguimiento del progreso.

Definir las áreas prioritarias y las partes **involucradas.**

En este punto es importante centrarse principalmente en la información *más sensible* que se maneja dentro de cada área, visualizandolas mayores brechas y oportunidades de violación que puedan ocurrir en la misma. El nombre y cargo de quién será la persona de contacto en dicha área también debe definirse.

Entonces, se debe crear una tabla en la que se identifique la siguiente información (en columnas) y, para llenarla, se sigan lassiguientes directrices.

1.1. No.: Es el ordinal del área prioritaria.

1.2. ÁREA PRIORITARIA: Es el área que, por la sensibilidad de la información que se mane-ja, debe ser protegida.

1.3. NOMBRE DEL INVOLUCRADO: Contiene el nombre de la persona que será la contraparte de seguridad de la información en cada área prioritaria.

1.4. CARGO: Contiene el cargo de la persona que será la contraparte de seguridad de la información en cada área prioritaria.

1.5. INFORMACIÓN SENSIBLE: Es una breve descripción de la información que debe ser protegida, indicando el por qué se la considera sensible.

1.6. BRECHA U OPORTUNIDAD DE VIOLACIÓN: Aquí se debe identificar las vulnerabilidades detectadas.

2. Realizar una evaluación del estado actual de la Seguridad de la información.

Para cada una de las áreas prioritarias definidas en la Columna 1.2., revisar cada uno de los 6 criterios de evaluación definidos enel numeral 2.1. Basar las calificaciones segúnel cumplimiento con un “sí” fuerte (5), un “no” fuerte (1) o valores intermedios.

Usar los siguientes criterios de puntuación de respuesta: 1 (totalmente en desacuerdo), 2 (en desacuerdo), 3 (neutral), 4 (de acuerdo), 5 (totalmente de acuerdo).

2.1. CRITERIOS DE EVALUACIÓN: Ingresar en filas los siguientes criterios:

2.1.1. Desarrollar y gobernar una cultura de seguridad saludable.

2.1.2. Establecer una línea base de control.

2.1.3. Instituir detección y respuesta resistentede vulnerabilidades.

2.1.4. Controlar el acceso sin crear un obstá-culo para la Institución.
2.1.5. Desarrollar y gobernar una fuerte culturade seguridad.
2.1.6. Gestionar el riesgo de seguridad de in-formación en la institución.

Ingresar en columnas, cuándo se efectúa la evaluación (3), y las observaciones, de existir.

HOY – PUNTUACIÓN (1 A 5): Evaluar la situación actual de cada criterio, desde el 2.1.1 hasta el 2.1.6.

2.3. + 3 MESES – PUNTUACIÓN (1 A 5): Evaluar la situación esperada de la fecha actuala 6 meses de cada criterio, desde el 2.1.1 hasta el 2.1.6.
2.4. + 6 MESES – PUNTUACIÓN (1 A 5): Evaluar la situación esperada de la fecha actuala 6 meses de cada criterio, desde el 2.1.1 hasta el 2.1.6.
2.5. OBSERVACIONES**:** Incluir observaciones que deban ser consideradas como parte de la evaluación.

Para otorgar la evaluación a cada uno de los criterios de evaluación del numeral 2.1, considerar los siguientes subcriterios (20),otorgándoles una nueva puntuación de 1 a 5, y para obtener la puntuación del criterio,calcular el promedio de las evaluaciones de lossubcriterios.

1.1.1. Desarrollar y gobernar una cultura de seguridad saludable: Definir la puntuación, para ello, obtener el promedio en base a los 20 subcriterios definidos a continuación. Se puede considerar implementar acciones en los próximos 3 o6 meses.
1.1.1.1. ¿La estructura de la gobernanza de la seguridad está bien alineada con la for- ma en que las Tecnologías de la Información - TI y la institución están organizados?
1.1.1.2. ¿La definición de seguridad de la información (misión, estructura y principios operativos) está recogida en el Reglamento Interno de la Institución y está enfuncionamiento?
1.1.1.3. ¿Se reúne regularmente un comité directivo de seguridad; asisten regular- mente a él representantes de seguridad, TI, administración corporativa con autoridad para firmar; y es eficaz para abordar cuestiones de seguridad multi- funcional y hacer avanzar los proyectos de seguridad?
1.1.1.4. ¿El comité directivo de seguridad concientiza de los riesgos a los directivos de la institución y sirve como un lugar útil para examinar los riesgos más im-portantes y las recomendaciones de tratamiento?
1.1.1.5. ¿Están las políticas, normas, procesos y procedimientos de seguridad actualiza- dos y las prácticas cotidianas de la institución los siguen?
1.1.1.6. ¿Existe presupuesto de seguridad y se lo ejecuta?
1.1.1.7. ¿Los directivos de la institución dan prioridad y apoyan la ciberseguridad (es de- cir, la consideran estratégica)?
1.1.1.8. ¿Proporcionan los directivos de la institución recursos para proyectos de seguridad y ayudan a hacer cumplir las políticas de seguridad?
1.1.1.9. ¿El líder de la seguridad de la información está incentivado a: a. ¿Mantener una comunicación regular con los líderes de las áreas críticas? b. ¿Mejorar sus habilidades de comunicación y la delos miembros de su equipo?
1.1.1.10. ¿El equipo de seguridad cuenta con proveedores definidos para casos críticos de afectación de las TI de la institución?
1.1.1.11. ¿El equipo de seguridad cuenta con una planificación de concienciación del usuario a la medida de la institución?
1.1.1.12. ¿Apunta la planificación de sensibilización y capacitación del usuarioa:

a. ¿Comunicarse de manera eficaz para lograr naturaleza de conciencia (sembrar en la mente ideas como «podemos hacer esto», «así es como otros han sido seguros y exitosos»)?
b. ¿Focalizar los programas de concienciacióna audiencias específicas?
c. ¿Coordinarlos programas con el liderazgo de las audiencias?
d. ¿Proporcionar formaciónespecífica para cada área?
e. ¿Reclutarlíderes entre el público objetivo y «entrenar a los entrenadores»?
f. ¿Proporcionar información o herramientas gratuitas que ayuden al personal y a sus familias mejorar la ciberseguridad en casa?
g. ¿Coordinar con la organizaciónde marketing interno programas de comunicación de ciberseguridad?
h. ¿Usarmedios de comunicación innovadores y entretenidos, productos o servicios?

1.1.1.13. ¿El programa de liderazgo o concienciación de seguridad mide por sí mismo si la conciencia y los programas de entrenamiento están mejorando:

a. ¿El comportamiento relacionado con la seguridad?
b. ¿Las actitudes y percepciones sobre el programa de seguridad?
c. ¿La comprensión de las políticas, herramientas y procedimientos (cognición y cumplimiento)? d. ¿Los resultados de la auditoría de cumplimiento?

1.1.1.14. ¿Se responsabilizan los directivos de las instituciones del riesgo de la información?
1.1.1.15. ¿Utilizan los equipos institucionales de

trabajo, TI y seguridad una terminología consistente para debatir el riesgo y criterios coherentes para evaluar el riesgo?

1.1.1.16. ¿Las partes interesadas acu- den al equipo de seguridad en busca deorientación o asesoramiento antes de tomar decisiones importantes que podrían crear riesgos?

1.1.1.17. ¿Se utilizan las evaluaciones de riesgos para priorizar los proyectos de seguridad, gestionar a terceros, o tomar otras decisiones?

1.1.1.18. ¿Se utiliza una metodología de análisis de riesgos cuantitativos?

1.1.1.19. ¿Se vigilan los problemas, riesgos, excepciones/aceptaciones y principales riesgos en un sistema de gestión de problemas, en una herramienta de gobernanza, riesgo y cumplimiento de la tecnología de la información y/o en un registro de riesgos?

1.1.1.20. ¿Se comunican regularmente los riesgos de la información sensible a los ejecutivos y a la Junta, y es el diálogo constructivo?

1.1.2. ***Establecer una línea base de control:*** Definir la puntuación, para ello, obtener el promedio en base a los subcriterios definidos a continuación (7). Se puede considerar implementar acciones en los próximos 3 o 6 meses.

1.1.2.1. ¿Tiene la institución un "marco de control" y/o un documento de "línea base de control" que enumere los objetivos de control para las TI y la institución?

1.1.2.2. ¿Tiene el equipo de seguridad una guía publicada que relacione los objetivos de control con las actividades de control requeridas para diferentes niveles de riesgo o diferentes situaciones (por ejemplo, clasificaciones de datos, uso de servicios de terceros)?

1.1.2.3. ¿Se ha mapeado la línea de base de control a los documentos de requisitos y las arquitecturas de solución para los sistemas operativos críticos en los en- tornos de TI y de seguridad?

1.1.2.4. ¿Se actualiza y se sigue la línea de basede control?

1.1.2.5. ¿Tienen los equipos de gestión de la TI,de seguridad un marco de responsabilidad compartida para ayudar a evaluar los servicios de terceros?

1.1.2.6. ¿Se especifica en un documento de arquitectura cómo deben ejecutarse los controles?

1.1.2.7. ¿Tiene la institución una función de auditoría para verificar que los controles funcionan?

1.1.3. Instituir detección y respuesta resistente a vulnerabilidades: Definir la puntuación, para ello, obtener el promedio en base a los subcriterios definidosa continuación (8). Se puede considerar implementar acciones en los próximos 3o 6 meses.

1.1.3.1. ¿Tiene la Institución creados estándares de registro (logs de los sistemas críti- cos)?

1.1.3.2. ¿Tiene la Institución un centro de operaciones de seguridad (SOC) y/o un proveedor de servicios de seguridad gestionada (MSSP)?

1.1.3.3. ¿Tiene la Institución un sistema de gestión de información y eventos de seguridad (SIEM)?

1.1.3.4. ¿Tiene la Institución un equipo de respuesta a incidentes de seguridad informática (CSIRT)?

1.1.3.5. ¿Tiene la Institución planes de respuesta a incidentes? a. ¿Se ha comprobado la eficacia de estos planes en incidentes o pruebas reales?

1.1.3.6. ¿Tiene la institución un inventario de activos y una evaluación del impacto institucional actual (BIA) que identifique los activos críticos?

1.1.3.7. ¿Tiene la institución un plan y programade continuidad de negocio y recuperación de desastres (BC/DR)?

1.1.3.8. ¿Se ha probado el plan BC/DR?

1.1.4. Controlar el acceso sin crear un obstáculo para la Institución: Definir la puntuación, para ello, obtener el promedio en base a los subcriterios definidosa continuación (8). Se puede considerar implementar acciones en los próximos 3o 6 meses.

1.1.4.1. ¿Tiene la Institución un equipo de gestión de identidad y acceso multifuncional?

1.1.4.2. ¿El equipo multifuncional se reporta o coordina con el equipo de seguridad?

1.1.4.3. ¿Dispone la Institución de modelos coherentes de políticas de acceso a las áreas principales y/o críticas?

1.1.4.4. ¿Tiene la Institución a alguien que traba-je en el gobierno de la información?

1.1.4.5. ¿Tiene la Institución un Director de Privacidad o un Director de información? ¿Oficial de protección de datos?

1.1.4.6. ¿Sabe el departamento de seguridaddónde está almacenada toda la información sensible?

1.1.4.7. ¿Son los derechos de acceso privilegiados (es decir, la cuenta de raíz o el dominio administrador está restringido a pequeños grupos de usuarios)?

1.1.4.8. ¿Se controla o vigila el acceso privilegia-do?

1.1.5. Desarrollar y gobernar una fuerte cul-tura de seguridad: Definir la puntuación, para ello, obtener el promedio en base a los subcriterios definidos a continuación (5). Se puede considerar imple-mentar acciones en los próximos 3 o 6 meses.

1.1.5.1. ¿Tiene la institución un entorno de seguridad de información simplificado y racionalizado?

1.1.5.2. ¿Existe una estrategia de seguridad de información publicada y actualizada?

1.1.5.3. ¿Se ha alineado la estrategia de seguridad con la estrategia de la Institución?

1.1.5.4. ¿Publica el equipo de seguridad de la información un catálogo de servicios de seguridad?

1.1.5.5. ¿Trabaja el equipo de seguridad en es-trecha colaboración con la administración de terceros para evaluar el riesgo de éstos en las primeras fases del pro- ceso de evaluación comercial?

1.1.6. Gestionar el riesgo de seguridad de información en el negocio*:* Definir la puntuación, para ello, obtener el promedio en base a los subcriterios definidos a continuación (10) basados en la ISO 31000. Se puede considerar implementar acciones en los próximos 3 o 6 meses.

1.1.6.1. ¿Se ha establecido el contexto interno y/o externo, esto es, calificar los riesgos y establecer si son de contexto interno o externo, entendiéndose por *contexto externo*, aquel riesgo que se deriva de factores culturales, sociales, políticos, jurídicos, reglamentarios, financieros, tecnológicos, económicos, o relativos a la competencia; y el riesgo de *contexto interno*, el relacionado con el capital, el tiempo, el recurso humano, los procesos, la estructura organizativa, las responsabilidades, las funciones, la estrategia, los procesos de toma de decisiones, entre otros?

1.1.6.2. ¿Se ha establecido el enfoque en la definición de los riesgos en la Institución sincronizándolo con los objetivos que se desea alcanzar?

1.1.6.3. ¿Se han identificado los riesgos específicos, reconocidos, descritos y ubicadosen una lista de ellos y de los eventos que los pueden generar, aumentar, acelerar, o, por el contrario, reducir o retardar?

1.1.6.4. ¿Se han analizado los riesgos, es decir,se han evaluado las causas y las fuentes de riesgos, sus consecuencias, negativas y positivas – que pueden existir –, y las probabilidades de que se produzcan tales consecuencias?

1.1.6.5. ¿Se han evaluado los riesgos sobre la base obtenida del análisis para ayudar a tomar decisiones?

1.1.6.6. ¿Se han tomado decisiones sobre el tratamiento a los riesgos, es decir, seha actuado y emprendido acciones que modifiquen el riesgo para aliviarlo, pre-venirlo, eliminarlo y cambiar su rumbo de afectación?

1.1.6.7. ¿Se ha comunicado y obtenido retroalimentación de la gestión de los riesgos, mediante la obtención de informacióncontinua e iterativa a través de diálogos,foros, debates, entre otros con las áreascríticas?

1.1.6.8. ¿Se ha implementado un plan de moni- toreo mediante un proceso continuo de verificación, supervisión y observación crítica, que pretende identificar cambios en la situación que pudiesen generarnuevos riesgos, o afectar la eficacia del plan de Gestión de Riesgos?

1.1.6.9. ¿Se realiza un análisis crítico, que es la actividad llevada a cabo para determinarla idoneidad, adecuación y eficacia del plan de Gestión de Riesgos?

1.1.6.10. ¿Se tiene implementado un pro-ceso de auditoría que alimente, monito- ree, supervise y analice en forma conti- nua el plan de Gestión de Riesgos, ya que los riesgos son dinámicos?

Definir objetivos de mejora (dentro de las áreas de enfoque prioritarias).

Hasta ahora se ha evaluado el estado actual dela seguridad de la información para cada una delas áreas prioritarias de la institución educativa.En cada área, se han evaluado 6 criterios en base a los respectivos subcriterios. En primer lugar, se debe identificar los subcriterios que obtuvieron una evaluación menor a 4, convertirlos en objetivos de mejora de cadacriterio de cada área prioritaria.

Así, para el área prioritaria establecida, parael criterio uno, determinar los subcriterios con evaluación menor a 4 y establecer:

2.1.1. El subcriterio transformado a objetivo u objetivos de mejora.

2.1.2. Las actividades, en donde se describelo que se va a realizar para cumplir el objetivo

2.1.3. El estado actual, en donde se ubica la evaluación inicial obtenida.

Se dispone de tres (3) meses para ejecutar las actividades y cumplir el objetivo propuesto.

Una vez que se han cumplido los objetivos paralos subcriterios mencionados, se procede a trabajar de la misma manera con los de estado actual 4 y finalmente con una revisión de losde estado actual

5 para controlar que no hayansido descuidados.

Este procedimiento se repite para los 5 criteriosde evaluación restantes en cada área prioritariaelegida.

Identificar métricas

Las actividades que se han realizado para cumplir los objetivos de mejora propuestos ahora se transforman en métricas cuantificables,medibles y/u observables, a los 3 y 6 meses.

Así, para el área prioritaria establecida, para el criterio uno, para los subcriterios con evaluaciónmenor a cuatro, para los objetivos de mejora establecidos se define:

3.1.1. El objetivo de mejora.
3.1.2. La métrica para determinar si el objetivode mejora se ha cumplido.
3.1.3. El valor de la métrica en la evaluación.
3.1.4. El valor de la métrica que se espera a los 3 meses de trabajo a partir de la evaluación.
3.1.5. El valor de la métrica que se espera a los 6 meses de trabajo a partir de la evaluación.

Si se han alcanzado o sobrepasado las métricas establecidas, se consideran como objetivos esperados cumplidos, caso contrario, se los sigue trabajando, estableciendo las causas por las que no se han alcanzado las métricas esperadas.

Nuevamente, este procedimiento se repite paralos 5 criterios de evaluación restantes en cada área prioritaria elegida.

Realizar seguimiento del proceso

En este punto, es necesario determinar si los

Un criterio de evaluación con puntajes muy bajos en las distintas áreas prioritarias ha sido mejorado. Si no se han enmendado según lo definido, es el momento para recurrir a consultorías y/o asesorías.

Los subcriterios que tienen estado actual menor a tres, deben ser mejorados al año como máximo. Los de puntuación cuatro (4) luego de un año y los de cinco revisados cada dos años.

El seguimiento consiste en repetir el proceso tal cual se lo efectuó para evaluar el estado actual de la seguridad de la información, pero para las áreas prioritarias definidas, para los seis criterios de evaluación, para los subcriterios cuyo estado actual esté en el rango dentro del cual se está mejorando.

RESULTADOS

El esquema planteado abarca una serie de criterios y subcriterios que conllevan a la estructuración de un plan de ciberseguridad aplicable a educación general básica en el Ecuador. Cada institución educativa, dependiendo de su contexto, lo debe adaptar para conseguir los resultados que se exponena continuación.

1. Estar informado, actualizado y alerta sobre la situación de la seguridad de la información a partir de la evaluación del estado actual de la institución educativa.
2. Conocer las herramientas para hacer frentea las vulnerabilidades, amenazas y riesgos por acción de los ciberdelincuentes.
3. Poder usar herramientas de protección en línea, muchas de las cuales otorgan la facilidad de probarlas por un tiempo y, si satisface las necesidades de la institución, se las puede adquirir a través de una licencia pagada.
4. Estimular el pensamiento crítico de los miembros de la comunidad educativa, al ser concientizados a través de las capacitaciones, de la importancia de las buenas prácti cas de la seguridad de la información.
5. Configurar la conexión a Internet para un uso seguro y controlado, regulando el ac- ceso a la información de manera segregadasegún el rol de cada persona.
6. Aprender acerca de las redes sociales, el buen uso y el impacto que puede tener la publicación indiscriminada de la información personal, familiar, institucional entre otros.
7. Entender el beneficio de los juegos y las aplicaciones. Sobre todo, ahora en la virtualidad, los docentes usan cotidianamente lo mencionado, para conseguir mantener la atención de los estudiantes durante períodos extendidos de tiempo frente al computador, lo que quiere decir que se ha roto el estigma de que los juegos son perjudiciales y las aplicaciones beneficiosas. En lo uno y lo otro hay excepciones.
8. Entender la violencia en línea. Se debe res-petar las formalidades del uso de Internet y seguirlas para no incurrir en un mal uso e irreverencia.
9. Desconfiar de los requerimientos dudosos. La ciberdelincuencia echa mano de los mé-todos menos esperados para perpetrar sus acciones maliciosas.
10. Invertir tiempo en planificar, ejecutar y moni-torear actividades relacionadas con la segu-ridad de la información.
11. Educar a la comunidad educativa para que, conociendo los peligros, tome conciencia y actúe a la defensiva de esta manera evite ser víctima de los ciberdelitos.

DISCUSIÓN

La herramienta proyectada en este artículo guarda relación con lo establecido por Aportes de la Segunda Reunión del Diálogo Virtual con Rectores de Universidades Líderes de AméricaLatina (2020), en el que se menciona comopróximos pasos de las universidades a continuar con la formación de las competencias digitales de los profesores por medio de la acreditación de saberes, tomando en consideración

las situaciones que se pueden presentar al usar herramientas digitales para clases en línea quepueden ser intervenidas por ciberdelincuentes, como ya ha ocurrido, para presentar aspectos que nada tienen que ver con las actividades académicas, colocando mensajes obscenos oataques de privacidad.

También se interrelaciona con el mismo artículoen el sentido que permite fortalecer la comunidadvirtual existente para incentivar la interacción entre las universidades, con el objetivo de que intercambien experiencias, recomendaciones y mecanismos de digitalización, pero en ambientes seguros, al usar el esquema de plandefinido en el presente trabajo.

El procedimiento descrito apoya directamente a universidades públicas y privadas, pequeñas o medianas que estén retrasadas en suadaptación a la coyuntura, desde el punto de vista de la seguridad de la información.

De la misma forma, este artículo guarda congruencia con lo señalado por Avellán Zambrano & Zambrano Bravo (2019) cuandose define que es importante considerar el tipo o nivel de vulnerabilidad dentro de los dominiosque consta un sistema distribuido, debido a que si no se controlan a tiempo, podrían llegara materializarse y provocar ataques en la Web o en el ciberespacio. Aquí se mencionan dos horizontes de tiempo, a los tres y seis meses.

Asimismo, para mantener el control en aspectosde ciberseguridad, es necesario implementar como política un monitoreo constante, para que a futuro los sistemas no sean objetivos de ataques, y para sus efectos estos controles de riesgos deberán ser correctivos y preventivos, coincidiendo nuevamente con Avellán Zambrano& Zambrano Bravo (2019).

CONCLUSIÓN

Al definir las vulnerabilidades de los sistemas se logra concientizar a los miembros de la comunidad educativa sobre la importancia de mitigar los riesgos, mejorando la seguridad del manejo de la información de los sistemas distribuidos.

La aplicación del esquema del plan propuesto en este documento permitirá a las instituciones educativas mejorar la seguridad en el manejo de la información en los sistemas que éstas manejan, mediante la aplicación de las técnicas y recomendaciones fruto de la investigación efectuada con las herramientas de análisis de vulnerabilidad.

En el Ecuador, aunque el acceso a internet ha registrado un elevado incremento durante los últimos 5 años, las evidencias muestran que la reflexión en este tema de ciberseguridad es aún incipiente y se requieren esfuerzos integrales para su institucionalización. Al menos en Ecuador, las estadísticas referentes aviolaciones a la seguridad han sido en su mayoría dentro del sistema financiero; agregando que, un incremento en sus cifras ha convertido a la ciberseguridad en un tema preocupante, especialmente para la banca ecuatoriana.

Sin embargo, debido al acrecentamiento de la educación online, las ciber amenazas hacia los miembros de las comunidades educativas se han incrementado.

Por tanto, las iniciativas que, mediante las aplicaciones de un plan de ciberseguridad aplicable a la educación general básica ecuatoriana, planteada por el Ministerio de Educación, apuntan a frenar el delito informáticoque ha provocado la afectación del covid-19 a lacomunidad educativa.

AGRADECIMIENTO

Este estudio se realizó en base al requerimiento solicitado por el Ministerio de Educación del Ecuador a las instituciones educativas porél reguladas. Dirijo mi agradecimiento a las personas que generaron esta iniciativa en la citada institución, que permitió concebir el presente trabajo.

REFERENCIAS BIBLIOGRÁFICAS

Aportes de la Segunda Reunión del Diálogo Virtual con Rectores de Universidades Líderes de América Latina. (2020). *La educación superior en tiempos de CO- VID-19.* Washington, D.C.: BID.

Avellán Zambrano, N., & Zambrano Bravo, M.(2 de mayo de 2019). *Repositorio Ds- pace*. Obtenido de Ciberseguridad y su aplicación en las instituciones de educa-ción superior públicas de Manabí: http:// repositorio.espam.edu.ec/xmlui/hand- le/42000/1032

Deloitte. (01 de junio de 2020). *COVID-19: emergencia también en ciberseguri- dad.* Obtenido de COVID-19: emergen- cia también en ciberseguridad: https:// www2.deloitte.com/es/es/pages/risk/ articles/covid-19-emergencia-tam- bien-en-ciberseguridad.html

EDUCAWEB. (08 de abril de 2020). *Artículos y noticias de actualidad.* Obtenido de Con-sejos para estudiar online en tiemposde COVID-19: https://www.educaweb. com/noticia/2020/04/08/consejos-estu- diar-online-tiempos-covid-19-19137/

Esguerra, L. (02 de enero de 2020). *Buguroo*. Obtenido de Adolescentes y ciber cri- men: Los motivos de estas conductas: https://www.buguroo.com/es/blog/ado- lescentes-y-ciberdelincuencia-el-efec- to-de-

la-desinhibicion-online

Kaspersky. (s.f.). *Centro de Recursos.* Obte-nido de Consejos para protegerte contrael cibercrimen: https://www.kaspersky. es/resource-center/threats/what-is-cy- bercrime

Ona Systems. (31 de diciembre de 2018). *Ona Systems*. Obtenido de Estrategias de Ciberseguridad para colegios: https:// www.onasystems.net/estrategias-ciber-seguridad-colegios/

Significados. (31 de octubre de 2017). *Gene-ral*. Obtenido de Significado de Plan de Acción: https://www.significados.com/plan-de-accion/