Diseño de las Políticas Principales para la Actuación del Centro De Respuesta a Incidentes Informáticos de La Universidad Nacional Abierta y a Distancia CSIRT-UNAD

Andrés Vázquez Núñez
Especialización En Seguridad Informática
Universidad Nacional Abierta y a Distancia 1, Colombia
avasquesn@unadvirtual.edu.co

Luis Fernando Zambrano Hernandez
Especialización En Seguridad Informática Universidad Nacional Abierta y a Distancia 2, Colombia
luis.zambrano@unad.edu.co

Resumen - En la actualidad, la sociedad está sumergiéndose en un entorno totalmente digital, ahora, las actividades cotidianas relacionadas con educación han venido tomando fuerza en entornos digitales usando como canal de comunicación Internet, esto conlleva a que procesos administrativos y académicos puedan desarrollarse de forma rápida y efectiva sin necesidad de realizar acciones de forma presencial, lo cual ha permitido ahorrar tiempo y esfuerzo.

No obstante, en la misma medida que avanza la digitalización en la Industria que hoy se denomina 4.0, también lo hace el cibercrimen, por lo que es necesario asegurar que la información de las personas y las empresas se encuentre protegida de tal forma que las mismas tengan la tranquilidad de realizar sus actividades y transacciones en un entorno ciber seguro.

Para ello, las Instituciones de educación deben contar con personas altamente capacitadas para responder ante cualquier ciber incidente que, desde su actuación ética, tenga como referente: políticas, procesos y procedimientos que brinden los lineamientos para que sus responsabilidades estén reguladas y cumplan con lo establecido.

En este sentido, El proyecto denominado "Propuesta para la Creación y Consolidación del Centro de Respuesta a Incidentes Informáticos de la Universidad Nacional Abierta y a Distancia CSIRT-UNAD"[1], define cuáles son esas políticas que soportaran los servicios ofertados por el CSIRT y en particular este proyecto aplicado denominado "Diseño de las Políticas Principales Para la Actuación del Centro de Respuesta a Incidentes Informáticos de la Universidad Nacional Abierta y a Distancia – CSIRT-UNAD", contribuye con la construcción de las políticas principales que pueden ser tomadas como referente para el funcionamiento del Centro de Respuestas a Incidentes Informáticos de la Universidad Nacional Abierta y a Distancia CSIRT-UNAD.

Abstract - At present, society is immersing itself in a totally digital environment, now, daily activities related to education have been gaining strength in digital environments using the Internet as a communication channel, this means that administrative and academic processes can develop quickly and effective without the need to perform actions in person, which has saved time and effort.

However, to the same extent that digitization advances in the Industry that today is called 4.0, so does cybercrime, so it is necessary to ensure that the information of people and companies is protected in such a way that they have the peace of mind of carrying out your activities and transactions in a cyber secure environment.

For this, educational institutions must have highly trained people to respond to any cyber incident that, from their ethical performance, has as a reference: policies, processes and procedures that provide the guidelines so that their responsibilities are regulated and comply with the established.

In this sense, the project called "Proposal for the Creation and Consolidation of the Center for Response to Computer Incidents of the National Open and Distance University CSIRT-UNAD", defines which are those policies that will support the services offered by the CSIRT and in particular this applied project called "Design of the Main Policies for the Action of the Center for Response to Computer Incidents of the National Open and Distance University - CSIRT-UNAD", contributes to the construction of the main policies that can be taken as a reference for the operation of the Computer Incident Response Center of the National Open and Distance University CSIRT-UNAD.

Palabras clave— ataque**,** ciberseguridad, CSIRT, incidente, respuesta, políticas.

Keywords **—** attack, cybersecurity, CSIRT, incident, response, policies.

I. INTRODUCCIÓN

Conceptos previos

Política: “Las políticas son planteamientos generales o maneras de comprender que guían o canaliza el pensamiento y la acción en la toma de decisiones de todos los miembros de la organización” [2]

CSIRT: Es un organismo o equipo de profesionales altamente capacitados que brinda los servicios de prevención, gestión y respuesta a incidentes de seguridad de la información a una comunidad o empresas [3]

Incidente de Seguridad: “Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazar la seguridad de la información” [4]

En este artículo se presenta como se seleccionaron y construyeron las políticas principales que pueden ser tomadas como referente para el funcionamiento del Centro de Respuestas a Incidentes Informáticos de la Universidad Nacional Abierta y a Distancia CSIRT-UNAD, abordando la identificación del ámbito de actuación, el reconocimiento de los lineamentos y normativas relacionadas con la seguridad de la información que la Universidad ha definido y la consulta de buenas prácticas aceptadas en el orden mundial, estándares y documentación propia de otros CSIRT.

Algunas de las temáticas relevantes que se abordan en el artículo son: la definición de incidente de seguridad, sus clasificaciones y su gestión, clasificación de información, protección de datos, retención, destrucción, divulgación y acceso a la información, uso apropiado de los sistemas y cooperación entre instituciones que participen en la investigación de incidentes de seguridad de la información.

II. DESARROLLO DEL ARTICULO

Desde hace algunos años, el sector educativo viene presentando dificultad en la gestión de la ciberseguridad respecto a su infraestructura tecnológica, casos como el de la Universidad de los Andes [5] y la Universidad el Bosque [6] las cuales han presentado afectaciones en el resguardo de la seguridad de la información generando incertidumbre en su comunidad y pérdidas económicas.

Las universidades vienen siendo cada vez más vulnerables debido al gran almacenamiento de datos confidenciales, al a poca capacidad de reacción frente a un ataque informático y a la falta de presupuesto y personal capacitado [6]. Un dato que genera alerta es el que presenta el Instituto tecnológico de Monterrey, indicando que los ataques dirigidos a instituciones educativas de Estados Unidos incrementaron en un 50% y que el foco para realizar acciones delictivas son los estudiantes.

Según los datos entregados en la novena cumbre latinoamericana de Kaspersky Lab durante el año 2019, se ha evidenciado que en América Latina se presentan 45 ataques informáticos por segundo, siendo los ataques más utilizados, el phishing, ramsomware y malware.

La necesidad de establecer estrategias que permitan mejorar la seguridad de la información en las Instituciones no es ajena a la Universidad Nacional Abierta y a Distancia. Desde hace varios años, la UNAD viene desarrollando capacidades tecnológicas que dan respuesta a los servicios de educación ofertados, pero a su vez, estos pueden ser blanco de un evento o incidente informático. Es por esto por lo que políticas que se vienen generando como el Acuerdo 039 del 3 de diciembre de 2019 y la propuesta de la Políticas del Marco de Referencia del Sistema de Gestión de Seguridad de la Información – SGSI, aportan en mejorar el ámbito ciberespacial en los cuales se desarrollan los objetivos misionales de esta institución.

El Centro de Respuestas a Incidentes Informáticos CSIRT-UNAD es unas estrategias propuestas para dar respuesta a eventos o incidentes informáticos que puedan presentarse al interior de la Universidad. El ámbito de actuación de este CSIRT es el académico, donde tiene como objetivo: Brindar apoyo para la reacción ante eventos o incidentes cibernéticos que permitan reducir su impacto en comunidades académicas. Tiene además como función la generación de documentos que prevengan y alerten a la comunidad objetivo.

Es por esto por lo que la necesidad de construir Políticas principales que brinden los lineamientos para la actuación de este Centro es una necesidad.

Al respecto, se realizó una consulta documental de los lineamientos existentes en la Universidad, identificando que se cuenta con diferentes resoluciones que sirven como base para la definición de las políticas, las cuales son:

Resolución No. 2945 Por la cual se reglamenta el uso de los servicios de tecnología informática y telecomunicaciones de la Universidad Nacional Abierta y a Distancia – UNAD

Resolución 2943: Por la cual se establece la política para la clasificación y el manejo de la información confidencial en la Universidad Nacional Abierta y a Distancia – UNAD

Resolución 2944: Por la cual se regulan las políticas de seguridad informática y el uso adecuado de la tecnología para el procesamiento de la información en la

Universidad Nacional Abierta y a Distancia – UNAD

Resolución 6018: Por la cual se modifica la Resolución 4815 de 2012, mediante la cual se establecieron políticas para la clasificación y el manejo de la información confidencial en la UNAD. (Derogada con la Resolución 4256 del 3 de marzo del 2015. Políticas Marco de Referencia del SGSI).

Resolución 5071: Por la cual se define la política de renovación tecnológica de la Universidad Nacional Abierta y a Distancia – UNAD.

Resolución 2110: Por la cual se crea el Sistema de Gestión Tecnológica –SIGETEC, de la Universidad Nacional Abierta y a Distancia –UNAD, y se conforma el Comité Estratégico del Sistema de Gestión Tecnológica y la Mesa Técnica para su operación.

Resolución 0190: Por medio de la cual se conforma el Grupo Funcional de Gestión Técnica de la Plataforma Tecnológica Integrada, de la Universidad Nacional Abierta y a Distancia - UNAD y se dictan otras disposiciones.

Resolución 156: Por el cual se derogan las resoluciones 972 del 31 de mayo de 2007, la 5282 del 8 de octubre de 2012 y se actualiza el sistema de gestión documental de la Universidad Nacional Abierta y a Distancia – UNAD.

Resolución 4793: Por la cual se expide la Política de Seguridad de la Información y Gestión Documental de la Universidad Nacional Abierta y a Distancia.

Resolución 5303: Por el cual se expide el código de ética y de buen gobierno de la UNAD

Resolución 6858: Por medio de la cual se modifica la estructura del comité técnico de gestión integral y MECI y se derogan las resoluciones 3943 de 2011 y 2054 de 2007.

Resolución 7966: Por el cual de modifica la resolución 6858 de 22 de agosto de 2014, por medio de la cual se conforma el SIG - UNAD, se establece la política integrada de gestión y se derogan las resoluciones 2271 de 2008, 2055 de 20074 y 02861 de 2010

Teniendo en cuenta lo anteriormente expuesto, para dar respuesta a las necesidades y requerimientos legales y contractuales de las actividades emanadas de los servicios del CSIRT se soporta la construcción de las políticas principales de este, con las políticas y resoluciones anteriormente presentadas y las políticas propuestas por algunas organizaciones que ofrecen servicios de ciberseguridad.

POLITICAS PRICIPALES PROPUESTAS PARA EL CSIRT-UNAD

A continuación, se presentan las políticas propuestas para el desarrollo de las actividades principales del CSIRT-UNAD

Política De Clasificación De Información: Establece los lineamientos, criterios y actividades a seguir para una adecuada clasificación de la información, con el fin de evitar todos los daños asociados al tratamiento inadecuado de la información, la cual se debe proteger según sus características, evitando de esta manera: fugas de información de datos personales o confidenciales del CSIRT, pérdida de competitividad por información privada mal administrada, errores en datos reportados a entidades críticas e indisponibilidad de insumos de información que alimentan los principales procesos productivos y administrativos.

Política De Protección De Datos: Define los lineamientos, criterios y actividades a seguir para una adecuada protección de datos personales recolectados por el CSIRT, con base en lo señalado en la ley 1581 de 2012 y el decreto reglamentario 1074 de 2020.

Política De Retención De Información: Define el tiempo en que se retendrá los datos recolectados por el CSIRT de acuerdo con su clasificación.

Política De Destrucción De Información: Establece los lineamientos, criterios y actividades a seguir para la eliminación de información y/o depuración de los medios que la contienen; cuando sea necesario o cuando ha cumplido o terminado su ciclo de vida; con el fin de evitar que la información sea recuperada, preservando su confidencialidad.

Política De Divulgación De Información: Establecer lineamientos acerca de la manera en que será divulgada la información, con base en la necesidad de conocerla por parte del receptor de los datos.

Política De Acceso A La Información: Establece los por medio de los que se podrá tener acceso a la información y quién debe acceder a la información con base en la criticidad de esta.

Política De Uso Apropiado De Los Sistemas Del Csirt: Define los controles de seguridad y requerimientos mínimos con los que deben contar los sistemas de información del CSIRT los cuales permitan restringir el uso de estos únicamente para las labores de la compañía.

Documento De Definición De Incidentes De Seguridad Y Política De Eventos: Cuenta con la definición de incidente de seguridad y establece una clasificación de los posibles incidentes de seguridad a los que se puede ver expuesto el CSIRT.

Política De Gestión De Incidentes: Norma la implementación del proceso de gestión de incidentes de seguridad de la información, para disponer de una capacidad de reacción y respuesta apropiada a los incidentes de seguridad de la información en el CSIRT.

Política De Cooperación: Establece las directrices para la cooperación con otras entidades, como empresas de seguridad informática y CSIRT que colaboren con las investigaciones de incidentes de seguridad de la información, sin afectar la confidencialidad, disponibilidad e integridad de los datos del CSIRT y/o sus clientes.

Política Del Cumplimiento De La Ética Y La Confidencialidad: Establece las directrices para la utilización adecuada de los recursos entregados, con base a una cultura de compromiso y honestidad, comprendiendo que la información suministrada debe ser manejada con confidencialidad y ética profesional, así como también fomentar la educación y cultura en los equipos de trabajo.

III. CONCLUSIONES

Es de gran relevancia manifestar que la identificación del ámbito de actuación del Centro de Respuesta a Incidentes Informáticos CSIRT-UNAD, el cual es el académico, denota la importancia de establecer lineamientos claros que permitan dar cumplimiento a los requerimientos legales y contractuales y por defecto a la realización de la misión propuesta.

El reconocer los lineamientos con los que la Universidad Nacional Abierta y a Distancia – UNAD cuenta para el tratamiento y la gestión de la información, son un insumo que

aportan la esencia de lo que la Universidad proyecta como ámbito ciberespacial, el cual permite la interacción de los múltiples actores que gestionan y hacen uso de forma regular de herramientas tecnológicas que facilitan articular el meta sistema institucional con nuevas tecnologías, siendo las políticas propuestas los lineamientos dados para la ejecución legal y contractual de las actividades.

La construcción de las políticas principales para las actuaciones del CSIRT-UNAD, son un aporte que contribuye en la mejora de la ciberseguridad del entorno digital de la Universidad. Estas contienen las decisiones y lineamientos que permitirán realizar actuaciones desde el profesionalismo y la ética que un profesional de esta disciplina debe seguir.

AGRADECIMIENTO

A Dios por colocar siempre a las personas correctas en mi vida para que me enseñen provechosamente y por darme las fuerzas para superar todos obstáculos e ir más allá de los límites que hay en mi mente, a mi esposa por apoyarme cada vez que la necesité.

REFERENCIAS

[1] Zambrano, L, Peña, H, Quintero, J, Moreno, S, (2020). Propuesta para la Creación y Consolidación del Centro de Respuesta a Incidentes Informáticos de la Universidad Nacional Abierta y a Distancia CSIRT-UNAD “Tecnologías exponenciales para la consolidación de la industria 4.0”. Recuperado de: https://hemeroteca.unad.edu.co/index.php/memorias/article/view/4205/4180

[2] Hidalgo Sánchez, N. D. J. (2016). Políticas institucionalizadas por DISENSA para incrementar franquicias en el país y en la cuidad de Machala ventajas y desventajas para los franquiciados.

[3] OEA. Definición. En: Buenas prácticas para establecer un CSIRT nacional. Washington, D.C. 2006. p. 13.

[4] ICONTEC. EJEMPLO DE ENFOQUES PARA LA CATEGORIZACIÓN Y CLASIFICACIÓN DE EVENTOS E INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN. En: GTC-ISO/IEC 27035. 2015. p. 3.

[5] EL ESPECTADOR, (2016). Anonymous ataca el sitio web de la Universidad de los Andes. Recuperado de: https://www.elespectador.com/actualidad/anonymous-ataca-el-sitio-web-de-la-universidad-de-los-andes-article-620617/

[6] Beltrán, G, (2021). Agencia de periodismo investigativo. Universidad del Bosque bajo ataque cibernético. Recuperado de: https://agenciapi.co/noticia/academia/universidad-del-bosque-bajo-ataque-cibernetico

[7] Bricker & Eckler LLP, (2015). Privacidad y protección de datos. Seminario de ciberseguridad 2015. Recuperado de: https://www.bricker.com/industries-practices/privacy-data-protection/insights-resources/resource/2015-cybersecurity-seminar-783