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"

Luis Fernando Zambrano Hernández
Especialización en Seguridad Informática
Universidad Nacional Abierta y a Distancia 1, Colombia
Luis.zambrano@unad.edu.co

John Freddy Quintero Tamayo
Especialización en Seguridad Informática Universidad Nacional Abierta y a Distancia 3, Colombia
John.quintero@unad.edu.co

Hernando José Peña Hidalgo
Especialización en Seguridad Informática
Universidad Nacional Abierta y a Distancia 2, Colombia
Hernando.pena@unad.edu.co

Sonia Ximena Moreno Molano
Especialización en Seguridad Informática Universidad Nacional Abierta y a Distancia 4, Colombia
sonia.moreno@unad.edu.co

Resumen A continuación se exponen los pasos propuestos para la creación y consolidación del Centro de Respuesta a Incidentes Informáticos de la Universidad Nacional Abierta y a Distancia - UNAD, que de ahora en adelante se denominará CSIRT-UNAD.

Se presenta la planificación para la creación del CSIRT-UNAD, con una mirada enfocada en los ámbitos de actuación y las partes interesadas. Además, se plantea cómo se debe constituir el CSIRT-UNAD a partir del marco institucional, teniendo en cuenta el Plan de Desarrollo Institucional, las políticas emanadas por la Universidad y todo el marco legal en que debe ceñir su desempeño.

Así mismo se presenta el alcance propuesto para el desarrollo de las actividades del CSIRT-UNAD teniendo en cuenta cuál será la comunidad objetivo, los servicios que proporcionará y la evolución que los mismos puedan presentar. De la misma manera se plantea la estructura del talento humano que será parte del centro, su estructura organizacional, sus funciones y responsabilidades para el desarrollo de sus actividades y la articulación de este equipo en la ejecución de procesos relacionado con las operaciones cibernéticas en pro de contribuir en el desarrollo de las actividades de I+D+I.

Como resultados obtenidos, se presenta el ámbito de actuación del CSIRT-UNAD, el como debe ser su desarrollo económico, los servicios con los que dará respuesta a las necesidades de ciberseguridad generadas al interior de la Universidad y la propuesta de políticas mínimas requeridas para el desarrollo de su capacidad misional

Palabras clave— Amenaza, ciberseguridad, equipo, gestión, riesgo, vulnerabilidad.

***Abstract*—** Below are the proposed steps for the creation and consolidation of the Computer Incident Response Center of the Universidad Nacional Abierta y a Distancia, which from now on will be called CSIRT-UNAD.

The planning for the creation of the CSIRT-UNAD is presented, with a focus on the fields of action and the interested parties, in addition, it is proposed how the CSIRT-UNAD should be constituted from the institutional framework, bearing in mind the development plan and the policies issued by the University and the entire legal framework that must be adhered to for its performance.

Likewise, the proposed scope for the development of the activities of the CSIRT-UNAD is presented, bearing in mind which will be the target community, the services it will provide and the evolution that they may present. In the same way, the structure of the human Talent that will be part of the Center, its organizational structure, its functions and responsibilities for the development of its activities and the articulation of this team in the execution of processes related to cyber operations in favor of contribute to the development of R & D & I activities.

***Keywords*—** Threat, cybersecurity, team, management, risk, vulnerability**.**

I. INTRODUCCIÓN

Conceptos Previos

CSIRT Académico: Equipo de respuesta que brinda soporte a comunidades académicas, de forma frecuente tiene la característica de aunar esfuerzos con otros CSIRT académicos con el fin de desarrollar actividades de investigación. (OEA, 2016)

Servicios de un CSIRT: Se relacionan de forma directa con su misión y sus comunidades objetivos, presentando las líneas de apoyo para la gestión de la gestión de incidentes cibernéticos. El CSIRT-UNAD, presenta tres líneas de servicio

- Servicios reactivos, siendo estos los que se realizar a partir de un evento de ciberseguridad, indeseado o inesperado (ESET, 2015).
- Servicios proactivos, se presentan como la información que se debe bridar que apoye en la protección de infraestructura tecnológica (ESET, 2015).

Actualmente las tecnologías de la información y la comunicación son adoptadas como base para cualquier actividad socioeconómica debido al crecimiento de las redes y a su convergencia (PLANEACIÓN, 2016), permitiendo gestionar la información de manera eficiente, eficaz y efectiva, mejorando tiempos en su tratamiento, proporcionado datos que pueden ser analizados y evaluados de forma automatizada. Estas tecnologías, aunque agilizan los procesos de tratamiento de la información personal u organizacional vienen presentando fallos en su diseño e implementación poniendo en exposición sistemas que gestionan la información ocasionando dificultad en su disponibilidad, perdida de su integridad y confidencialidad, tal como lo indica el CAI virtual de la Policía Nacional donde Colombia en 2018 presenta un incremento del 28,3% de ataques informáticos en relación al 2017, lo que puede considerarse como la mutación del escenario físico al escenario virtual (CaiVIrtual, 2017).

La necesidad de atender riesgos asociados con la información que las organizaciones del sector académico generan en su qué hacer, logrando plantear a la Universidad Nacional Abierta y a Distancia la necesidad de proyectar una unidad estratégica destinada al

apoyo para la recepción, análisis, gestión y respuesta a reportes de incidentes relacionados con seguridad informática, a partir del fortalecimiento y adecuación de su infraestructura tecnológica y la creación de un Centro de Respuesta a Incidentes Cibernéticos "CSIRT-UNAD" que permita optimizar los procesos de I+D+i.

La propuesta para el mejoramiento de la infraestructura tecnológica y equipamiento para el desarrollo de actividades de CTeI se fundamenta en poder reducir la probabilidad y afectación de incidentes informáticos que comprometan las tecnologías de la información y la comunicación de la UNAD, de esta forma se contribuye en proporcionar ejecución a la meta 2021 propuesta en el Plan de Desarrollo de la UNAD 2019-2023, que propone la creación del Sistema de Operación de Seguridad Informático - SOC, teniendo como fundamento la resolución 4256 de marzo 3 de 2015 donde se definen las políticas del marco de referencia del SGSI y que enfatiza en el Artículo 2 que: "Esta política aplica para todos los procesos y procedimientos del sistema integrado de gestión de la universidad, así como a todas las actuaciones administrativas que desarrollen sus distintas unidades, por intermedio de sus funcionarios administrativos, cuerpo docente o contratistas" UNAD. (2018).

El artículo tiene como objetivo mostrar la Propuesta para la Creación y Consolidación del Centro de Respuesta a Incidentes Informáticos de la Universidad Nacional Abierta y a Distancia CSIRT-UNAD

II. DESARROLLO DEL ARTICULO

A. Centro de Respuesta a Incidentes Cibernéticos CSIRT-UNAD

CSIRT, por su sigla en inglés: Computer Security Incident Response Team, es un equipo que da respuesta a incidentes de seguridad cibernética. (http://www.first.org).

En el contexto de la ciberseguridad, se presentan otros tipos de equipos que contribuyen en dar respuesta a posibles eventos o incidentes informáticos. Entre ellos:

- SOC: Centros de operaciones de seguridad
- CERT: Equipos de respuesta ante emergencias informáticas

A continuación, en la figura 1, se visualiza una posible asociación entre CERT, SOC y CSIRT donde la prevención, la respuesta y la compresión muestran líneas de acción que intervienen en cada uno de los equipos:

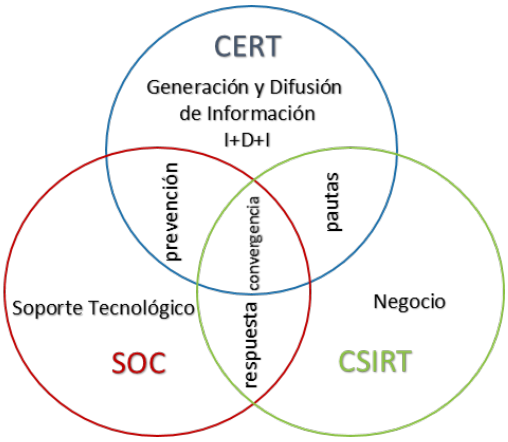

Figura 1 Similitudes Entre Equipos de Respuesta.
Fuente: («Certs, Csirts And Socs After 10 Years From Definitions», 2018)

El Registro de Direcciones de Internet de América Latina y Caribe – LACNIC, presenta la relación en CSIRTS's como la alianza estratégica que se debe generar para facilitar apoyo en el asesoramiento, solución a incidentes y la difusión de conocimiento de los temas trabajados en cooperación. También indica que es preciso establecer relaciones de apoyo, teniendo claro la información que se debe compartir y si la misma puede ser divulgada o no. (LACNIC2015, 2015).

Desde el análisis a partir de una matriz DOFA, Tabla 1, se plantean las Fortalezas, Amenazas, Oportunidades y Debilidades que la UNAD presenta en el momento de pensar en la Consolidación del CSIRT-UNAD.

Tabla 1:Matriz de Fortalezas, Amenazas, Oportunidades y Debilidades del CSIRT-UNAD

Amenazas	**Oportunidades**
Equipos tecnológicos que serán devaluados y obsoletos a corto y mediano plazo. Desaceleración de la economía	Desarrollar una línea de acción para la UNAD. Generar alianzas con otras instrucciones académicas para desarrollar procesos de I+D. Impactar en comunidades a partir de la difusión de información de Ciberseguridad, hasta un proyecto de interés general. Colombia no presente hasta el momento un Centro de respuesta académico. Se presentan 14 competidores en el mercado.
Fortalezas	**Debilidades**
Contar con un respaldo de atención a incidentes para la UNAD. Generar procesos de educación y cultura propuesto para el talento humano del CSIRT-UNAD Contar con talento humano calificado para dar respuesta a eventos o incidentes.	Experiencia. Reconocimiento de trabajo de un CSIRT. No se otorga la relevancia a la prevención en Ciberseguridad en sectores público-privados y por la comunidad en general. Presupuesto.

Fuente: Los Autores

B. Mapa de ruta para el diseño e implementación del CSIRT-UNAD

El diseño del mapa de ruta representado en la Figura 2, para la consolidación del Centro de Respuesta a Incidentes Informáticos de CSIRT - UNAD, se estructura teniendo en cuenta lo estipulado por la Organización de los Estados Americanos, la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), El Instituto de Ciberseguridad de España INCIBE y lo propuesto en el Manual para la Seguridad Informática y de Respuesta al Incidente - Equipos (CSIRT) de la Universidad de Carnegie Mellon, quienes presentan pautas para el diseño y consolidación de un CSIRT desde:

1. Planificación y creación del CSIRT-UNAD
2. Instalaciones e Infraestructura e Tecnológicas
3. Cierre

Figura 2. Mapa de Ruta Propuesto para la Implantación del CSIRT-UNAD

Fuente: Los autores

III. INNOVACIÓN TECNOLÓGICA

A. Ámbito de actuación del CSIRT-UNAD

El ámbito de actuación propuesto para el CSIRT-UNAD es de orden Académico, este 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 como se puede apreciar en la Figura 3.

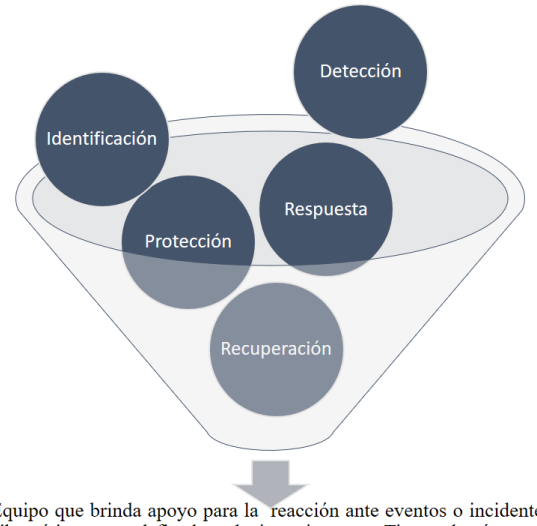

Figura 3: Esquema de CSIRT Académico, CSIRT-UNAD
Fuente: Los autores

El papel que desempeñará el CSIRT-UNAD, es lograr ser el primer Centro de Respuestas a Incidentes Informáticos Académico de Colombia, buscando generar impacto en universidades, institutos de educación superior, instituciones de educación para el trabajo y el desarrollo humano, colegios públicos y privados, en general a comunidades académicas que requieran de apoyo humano y tecnológico para proporcionar soluciones a dificultades emanadas de la ciberseguridad.

B. Definición del Modelo Financiero

Aunque el CSIRT-UNAD se constituye con el fin de establecer cumplimiento a lo planteado en el Plan de Desarrollo de la UNAD 2019 – 2023, el modelo económico para el CSIRT-UNAD se presente teniendo en cuenta el costo de inversión, el Retorno de Inversión – ROI y la propuesta del catálogo de servicios como se demuestra en la Tabla 2, Tabla 3, tabla 4, Tabla 5 y Tabla 6.

A continuación, se relaciona propuesta del catálogo de servicios del CSIRT-UNAD

Tabla 2: Soluciones de seguridad para la gestión de incidentes

Servicio	Etapa	Descripción	Productos
Gestión de incidentes	Prevención	Generación de Alertas: Valoración de eventos según su importancia y gravedad para su envío a los Gestores del CSIRT	SIM / SEM
	Detección	Análisis de Incidentes: Identificación y análisis de los eventos	SIEM
	Contención y respuesta	Soporte de Respuesta a Incidentes: Envío de documentación técnica frente a cómo reducir el evento o el impacto de llegar a presentarse el incidente, que permita	Monitoreo y reporte

Servicio	Etapa	Descripción	Productos
		generar su recuperación.	

Fuente: Los autores

Tabla 3: Soluciones de seguridad para la gestión de vulnerabilidades

Servicio	Etapa	Descripción	Productos
Gestión de Vulnerabilidades	Descubrimiento	Identificación de los activos de información requeridos para la verificación de vulnerabilidades.	Escáner de vulnerabilidades
	Detección y análisis	Recopilar la información relacionada con las vulnerabilidades presentadas en los activos de información	Monitoreo
	Clasificación	Se priorizan según su criticidad y vulnerabilidades descubiertas, cada uno de los activos de información.	Parcheo de vulnerabilidades
	Cierre de vulnerabilidades	Se parchan de manera física o virtual las vulnerabilidades descubiertas en los activos de información	Ethical Hacking

Fuente: Los autores

Tabla 4: Soluciones de seguridad en formación y concienciación

Servicio	Etapa	Descripción	Productos
Formación y concienciación	Formación en materia de Ciberseguridad (postgrados y educación continua)	Oferta de programas de posgrado y de educación continua en Ciberseguridad y seguridad informática	Campus Virtual
	Sensibilización y concienciación	Generar y mantener actualizados los boletines a partir de la estructura propuesta para la presentación de los anuncios	Piezas gráficas de sensibilización
	Certificación de normativa	Son servicios orientados a facilitar a las empresas y organizaciones la adecuación de cumplimiento normativo en materia de seguridad y obtención de certificados en estas normativas.	Normas

Fuente: Los autores

Tabla 5: Soluciones de seguridad en acompañamiento para el cumplimiento legal

Servicio	Etapa	Descripción	Productos
Cumplimiento Legal	Consultoría Legal	Consultoría legal en temas de Ciberseguridad	Jurídico
	Herramientas de Cumplimiento legal	Son herramientas destinadas a facilitar el cumplimiento legal, aplicable en materia de seguridad de la información o	Configuración y parametrización

Servicio	Etapa	Descripción	Productos
		protección de datos personales	
	Herramientas de borrado seguro	Herramientas para el borrado y la destrucción de información de forma segura y cumpliendo con la normativa vigente.	Borrado / Destrucción certificada

Fuente: Los autores

Tabla 6: Soluciones de seguridad para el acompañamiento de auditorías técnicas

Servicio	Etapa	Descripción	Productos
Auditorías técnicas	Auditoría Forense	Son servicios posteriores a un evento o incidente de seguridad, y están orientados a identificar las causas que lo produjeron.	Forense
	Hacking ético	Son actividades de auditoría que permiten identificar las vulnerabilidades de sistemas y aplicaciones, así como otros agujeros de seguridad.	Distribuciones de Seguridad
	Contingencia y continuidad	Son herramientas cuyo objetivo es planificar planes de actuación y contingencia destinados a mitigar el impacto provocado por cualquier incidente de seguridad,	Programas y Planes

Fuente: Los Autores

C. Beneficios de la Implantación del CSIRT

La importancia de la consolidación del CSIRT-UNAD además de gestionar de manera preventiva los servicios propios que emanan de su misión, gira entorno a la necesidad de promover espacios que permitan posicionar a la Universidad Nacional Abierta y a Distancia UNAD como una organización que contribuya en la divulgación de información y prestación de servicios para la buena gestión de la seguridad de la información, impactando en tres factores fundamentales descritos en la Tabla 7:

- Económico
- Relaciones publicas
- Legal

Tabla 7: Impacto económico, legal y de relaciones públicas

Sector	Impacto
Económicos	Permite reducir el tiempo requerido para la gestión de un evento o incidente cibernético, impactando en la perdida en tiempos de productividad
Relaciones Públicas	Reduce la exposición del activo intangible del nombre de la comunidad objetivo, favoreciendo el prestigio y buena imagen, así como la garantía de mostrar procesos seguros en la gestión de la información. A partir de los reportes de alertas e investigación se da a conocer el nombre de la UNAD, favoreciendo al sector externo manteniéndole al tanto de los avances en detección y prevención de incidentes relacionados con Ciberseguridad

Legales	Dar cumplimiento a los lineamientos legales y contractuales con las partes interesadas (sector público y privado) Contar con el soporte para las actuaciones legales relacionadas con incidentes de seguridad de la información

Fuente: Los autores

Otras de las ventajas de consolidar el Centro de Respuestas Incidentes Cibernéticos, son las que plantea la Agencia Europea de Seguridad de las Redes y de la Información (ENISA, 2006) las cuales se relacionan a continuación:

- Disponer de una coordinación centralizada para las cuestiones relacionadas con la seguridad de las TI dentro de la organización (punto de contacto).
- Reaccionar a los incidentes relacionados con las TI y tratarlos de un modo centralizado y especializado.
- Tener al alcance de la mano los conocimientos técnicos necesarios para apoyar y asistir a los usuarios que necesitan recuperarse rápidamente de algún incidente de seguridad.
- Tratar las cuestiones jurídicas y proteger las pruebas en caso de pleito.
- Realizar un seguimiento de los progresos conseguidos en el ámbito de la seguridad.
- Fomentar la cooperación en la seguridad de las TI entre la comunidad objetivo (sensibilización).

D. Alcance del CSIRT-UNAD

El CSIRT-UNAD, estará en la capacidad de apoyar procesos de detección, identificación, alertamiento, respuesta, recuperación, protección de amenazas y eventos o incidentes informáticos presentados al interior de la Universidad y a mediano plazo en organizaciones públicas o privadas del país, ofertando servicios reactivos asociados con la gestión de incidentes, la recuperación de ataques informáticos, la respuesta a artefactos maliciosos y servicios proactivos de primer nivel y segundo nivel en el monitoreo y alertamiento para detectar eventos de inseguridad que permitan fomentar **I+D** y la difusión de la información relacionada con la Ciberseguridad.

Adicionalmente, el CSIRT-UNAD se convierte en una unidad que apalanca el relacionamiento externo y le permite a la UNAD ampliar su marco de acción en el contexto de la responsabilidad social y el compromiso misional. Esto se logra al proyectar el CSIRT-UNAD como una oportunidad para apoyar las dinámicas de las microempresas, las pequeñas y medianas empresas, las grandes empresas y las infraestructuras críticas del país como un aliado estratégico, donde la responsabilidad social, la ética y los objetivos de desarrollo sostenible se involucran para dar como resultado una buena gestión de la información y procesos de educación y cultura en Ciberseguridad impactando a sus comunidades objetivo, contribuyendo en el crecimiento y desarrollo socioeconómico de Colombia.

E. Comunidad Objetivo

Se presenta como comunidad objetivo:

- Sector Académico.
- Microempresas: entre 1 y 10 empleados.
- Pequeñas empresas: entre 11 y 49 empleados.
- Mediana empresa: entre 100 y 500 empleados.
- Grandes empresas: más de 500 empleados.

- Infraestructuras críticas: Empresas con activos esenciales que prestan funcionamiento para la sociedad y la económica. (En Colombia se catalogan 13 tipos de infraestructura crítica)

A continuación, se presenta en la Tabla 8 la dependencia y asociación del CSIRT-UNAD con sus comunidades objetivo, vista desde un entorno digital seguro:

Niveles para identificar qué dependencia tienen las comunidades objetivo a partir de su infraestructura

Tabla 8: Niveles para identificar dependencias.

Dependencia Baja
Usa de computadores para trabajos administrativos Usa bases de datos de forma local Usa internet para realizar búsquedas de información Usa correo electrónico como una canal más de comunicación Puede contar con una página web informativa Tiene establecida una red de datos local para compartir procesos administrativos
Dependencia Media
Usa herramientas colaborativas para la gestión del modelo de negocio • Procesos • Talento Humano • Gestión de clientes Usa Internet como herramienta de mercadeo para potencializar el negocio, con el fin de cumplir las actividades planeadas Cuenta con servidor de correo configurado en su red o sub contratado Se hacen copias de seguridad en sitios remotos para salvaguardar la información Usa la red local para compartir procesos administrativos o información utilizando como infraestructura servidores propios La página web presenta contenido dinámico y actualizado Pueden hacer uso de dispositivos móviles o portables para tener acceso a la información a través de la red corporativa
Dependencia Alta
Se hace uso de diferentes tipos de red para desarrollar su modelo de negocio • Internet • Intranet • Extranet Puede contar con plataformas o sistemas de ventas en internet Realiza intercambios de forma electrónica para dar desarrollo al modelo de negocio • Contratación • Facturación Hace uso de herramientas colaborativas haciendo uso de sus plataformas web Cuneta con talento humano para resolver eventos o incidentes informáticos Dispone del recurso para seleccionar herramientas de trabajo digital para solventar sus necesidades

Elaboración propia

F. Análisis Político, Económico, Social y Tecnológico - PEST

El análisis PEST, mediante la Figura 4 permite identifica el impacto que puede tener el CSIRT-UNAD teniendo presente que este nace des sector académico y que su función va a ser la cooperación y la colaboración con sus comunidades objetivos.

Figura 4 Análisis PEST
Fuente: Los autores

G. Estructura Organizacional

En la Figura 5 se puede observar la estructura organizacional propuesta para el Centro de Respuestas a Incidentes Cibernéticos CSIRT-UNAD, se presenta teniendo en cuenta el Metasistema Unadista, ubicándolo en su sistema funcional, el cual tiene como objetivo garantizar la sostenibilidad, modernización y calidad del modelo de gestión.

Figura 5: Estructura organizacional del CSIRT-UNAD

Fuente: Los autores

H. Propuesta de Formación

Para el desarrollo de las actividades propuestas en los servicios del CSIRT, el talento humano debe estar en constante proceso de educación, entrenamiento y capacitación.

I. Diseño Locativo del CSIRT-UNAD

En la Figura 6, se presenta una proyección de la estructura básica del Centro de Respuestas Incidentes Cibernéticos CSIRT-UNAD. Como recomendación, las instalaciones locativas del CSIRT-UNAD deben estar en un lugar diferente al sitio que se pretende resguardar. Para el caso el sitio debe ser diferente a la sede José Celestino Mutis de la ciudad de Bogotá

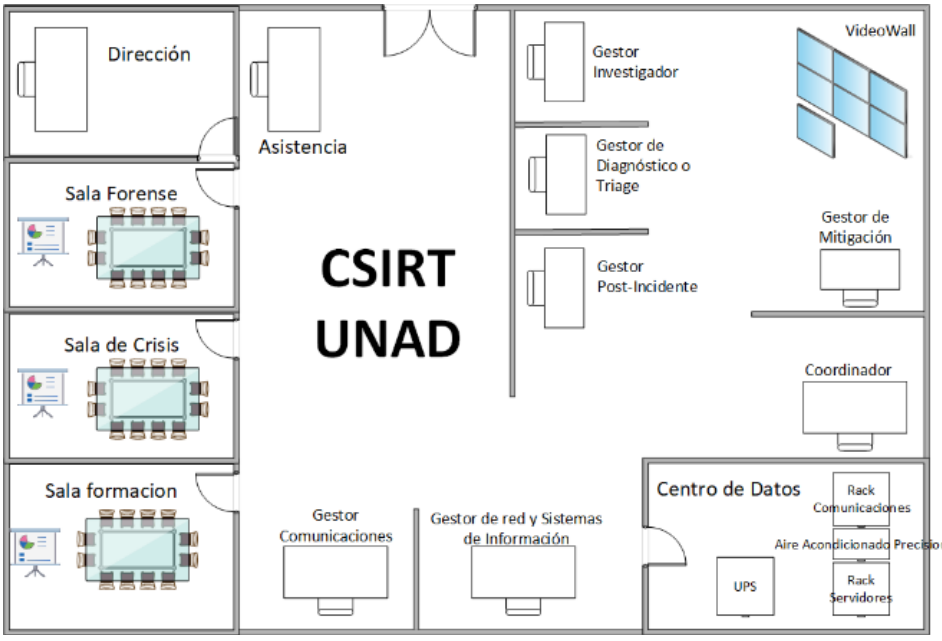

Figura 6: Instalaciones mínimas del CSIRT

Fuente: Los autores

J. Políticas Mínimas Obligatorias

Las actividades desarrolladas por el CSIRT-UNAD, deben estar alineadas a las políticas de la universidad, esto con el fin de integrar las directrices institucionales para garantizar la sostenibilidad y la mejora continua del Sistema Integrado de Gestión. También para tener clara la actuación ética de cada uno de los integrantes del Equipo. A continuación, se plantean algunas políticas mínimas obligatorias con las que el CSIRT-UNAD debe iniciar sus actividades.

Política de clasificación de información: Define los criterios para la clasificación y el acceso a la información. Esta debe contener una introducción, la gestión del control de acceso, la interacción con terceros, la gestión de la seguridad física y consideraciones para la gestión de información confidencial.

Política del Cumplimiento de la Ética y la Confidencialidad: Hace referencia al cumplimiento del código de ética con el que se orienta el equipo de trabajo y la confidencialidad que se debe dar a las acciones desarrolladas al interior del CSIRT.

Política de protección de datos: Presenta el derecho que tiene todas las personas para conocer, actualizar y rectificar la información recogida y almacenada en bases de datos.

Política de clasificación de los datos: define los criterios que se deben tener presenta para la clasificación, disposición y destrucción de la información. Esta debe contener como mínimo una descripción, control de acceso, la interacción con terceros, la seguridad física y consideraciones especiales relacionadas con la información confidencial.

Política sobre el acceso a la información: Presenta la forma de acceder a la información, el uso que se debe dar a la misma, la clase de información y su naturaleza, esta debe contener como mínimo una descripción, control de acceso, la interacción con terceros, la seguridad física y consideraciones especiales relacionadas con la información confidencial.

Políticas de uso apropiado de los sistemas del CSIRT: Esta política debe indicar las normas para la manipulación y uso de los equipos de parte del recurso humano del CSIRT, indicando si los miembros del equipo son sus administradores y dejando claro que el uso de estos no es personal. Debe contener como mínimo una descripción, su objetivo y consideraciones para el uso de información confidencial.

Definición de incidentes de seguridad y política de eventos: Presenta los criterios permitidos ya adecuados para dar tratamiento a un evento o incidente cibernético, esta debe contener como mínimo una descripción, una propuesta de clasificación de notificaciones, como se podría interactuar con terceros y algunas consideraciones especiales respecto a información confidencial.

Política de gestión de incidentes: Presenta la forma o los medios que se pueden utilizar para dar tratamiento o manejo a un incidente. Esta debe contener como mínimo, una descripción, la forma de la administración del riesgo, la forma de interacción con los terceros, la reserva de la información y algunas consideraciones especiales respecto al tratamiento de información confidencial.

Política de cooperación y de comunicación externa: Indica las normas para realizar el intercambio de comunicaciones con organizaciones externas, esta debe contener

como mínimo una descripción, control de acceso, la interacción con terceros, la seguridad física y consideraciones especiales relacionadas con la información confidencial.

Política de Seguridad: Hace referencia a las directrices y objetivos de seguridad planteados por la organización. Esta debe contener el alcance, sus objetivos, las responsabilidades del equipo de trabajo según el acceso que tienen a la información y una descripción de los elementos involucrados.

IV. CONCLUSIONES

Sin duda alguna, el CSIRT-UNAD se consolida como una gran apuesta de la Universidad Nacional Abierta y a Distancia, para el logro del aseguramiento de su entorno digital; para ello la Universidad se prepara generando las condiciones administrativas, de gestión, infraestructura y presupuestales que permitan consolidar un equipo técnico y humano, capaz de responder al reto de carácter científico, tecnológico y de innovación que implica la apertura y puesta en marcha de este tipo de centros.

De otro lado, el poder aportar capacidad de respuesta al sector académico, con la finalidad de cooperar para el tratamiento y respuesta a incidentes, como aliados en la operación, así como en el proceso académico y de investigación derivado de ella, marca un hito para la academia en Colombia.

En última instancia, y no por eso menos importante, la posibilidad de apoyar procesos de aseguramiento y respuesta a los diferentes sectores económicos en las regiones, como un ejercicio de extensión e impacto en los territorios donde hace presencia la UNAD, pone de manifiesto el derrotero misional de la institución: ¡Más UNAD, más PAÍS!

AGRADECIMIENTO

Agradecimiento de los autores a los Ingenieros Andrés Ernesto Salinas Duarte, Claudio Camilo González Clavijo y Christian Reynaldo Angulo Rivera, por su apoyo, acompañamiento y recomendaciones en este proyecto que impacta nuestro desarrollo integral y profesional y en la mejora de un entorno digital seguro para la Universidad Nacional Abierta y a Distancia.

REFERENCIAS

810-Guia_Creacion_CERT-sep11.pdf. (s. f.). Recuperado 13 de febrero de 2020, de https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-sep11.pdf

2016 - Buenas Practicas CSIRT.pdf. (s. f.-a). Recuperado 1 de noviembre de 2019, de https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

About FIRST. (s. f.). FIRST — Forum of Incident Response and Security Teams. Recuperado 23 de noviembre de 2019, de https://www.first.org/about

CERTs, CSIRTs and SOCs after 10 years from definitions. (2018, marzo 25). Security Boulevard. https://securityboulevard.com/2018/03/certs-csirts-and-socs-after-10-years-from-definitions/

CSIRT Framework Development SIG. (s. f.). FIRST — Forum of Incident Response and Security Teams. Recuperado 23 de noviembre de 2019, de https://www.first.org/global/sigs/csirt

Enisa. (2006). CÓMO CREAR UN CSIRT PASO A PASO [Guía]. https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullReport

FIRST — Forum of Incident Response and Security Teams. (s. f.). FIRST — Forum of Incident Response and Security Teams. Recuperado 23 de noviembre de 2019, de https://www.first.org/education

García et al. - Jaime Alberto Leal Afanador Rector.pdf. (s. f.). Recuperado 13 de febrero de 2020, de https://informacion.unad.edu.co/images/PLAN-DESARROLLO-2019-2023-f.pdf

Standards. (s. f.). FIRST — Forum of Incident Response and Security Teams. Recuperado 23 de noviembre de 2019, de https://www.first.org/standards

Internet Crime Report 2019. (2020). Recuperado 24 March 2020, de https://pdf.ic3.gov/2019_IC3Report.pdf

2016—Buenas Practicas CSIRT.pdf. (s. f.). Recuperado 28 de marzo de 2020, de https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

Articles-5482_G21_Gestion_Incidentes.pdf. (s. f.). Recuperado 23 de marzo de 2020, de https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

García, C. A., Perlaza, L. Y., Guzmán, L. L., Rodríguez, E. G., Torres, L. E. S., Mateus, N. R., & Pacheco, P. I. (s. f.). Jaime Alberto Leal Afanador Rector. 14, 122.

GuiaICC.pdf. (s. f.). Recuperado 28 de marzo de 2020, de https://acis.org.co/archivos/Conferencias/2016/GuiaICC.pdf

Impacto de los incidentes de seguridad digital en Colombia 2017 | Publications. (s. f.). Recuperado 28 de marzo de 2020, de https://publications.iadb.org/publications/spanish/document/Impacto-de-los-incidentes-de-seguridad-digital-en-Colombia-2017.pdf

Manual_basico_sp.pdf. (s. f.). Recuperado 28 de marzo de 2020, de https://warp.lacnic.net/wp-content/themes/warpnew/docs/manual_basico_sp.pdf

Normograma—Universidad Nacional Abierta y a Distancia UNAD - Educación Virtual. (s. f.). Recuperado 28 de marzo de 2020, de https://informacion.unad.edu.co/control-interno/documentos/normograma

Objetivos de Desarrollo Sostenible | PNUD. (s. f.). UNDP. Recuperado 28 de marzo de 2020, de https://www.undp.org/content/undp/es/home/sustainable-development-goals.html

Quintero, C. A. (s. f.). EQUIPO DE POLICÍA NACIONAL. 36.

Quintero—EQUIPO DE POLICÍA NACIONAL.pdf. (s. f.). Recuperado 23 de marzo de 2020, de https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Real Academia Española. Diccionario Usual. (s. f.). Recuperado 23 de marzo de 2020, de http://lema.rae.es/drae2001/srv/search?id=9nhM8bTF1DXX2pAkGvA4

Incibe 2016. Recuperado de https://www.incibe.es/sites/default/files/cont

enidos/guias/doc/taxonomia_ciberseguridad.pdf

Incibe (2017), que es una DMZ y cómo te puede ayudar aproteger tu empresa. Recuperado de: https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa

ITU. (2017). Global Cybersecurity Index Recuperado de https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

https://warp.lacnic.net/wp-content/themes/warpnew/docs/manual_basico_sp.pdf