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 VÁSQUEZ NÚÑEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2021

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 VÁSQUEZ NÚÑEZ

PROYECTO DE GRADO

DIRECTOR: LUIS FERNANDO ZAMBRANO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2021

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Bogotá D.C. y 08 de octubre de 2021

DEDICATORIA

A Dios y a mi esposa.

AGRADECIMIENTOS

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 y por sacrificar tiempo valioso juntos para conseguir este logro.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág

LISTA DE FIGURAS

RESUMEN

El presente proyecto aplicado busca diseñar las principales políticas que brinden los lineamientos de actuación del Centro de Respuesta a Incidentes Informáticos de la Universidad Nacional Abierta y a Distancia – CSIRT-UNAD, lo anterior, por medio de la identificación del ámbito en el cual actuará el CSIRT, el reconocimiento de los lineamentos y normativas que se relacionan con la seguridad de la información que la universidad ha definido, así como, la consulta de buenas prácticas aceptadas en el orden mundial, estándares y documentación propia de otros CSIRT en varios países como Estados Unidos, España, entre otros.

Algunas de las temáticas relevantes que se abordan en el proyecto 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.

PALABRAS CLAVE

Ataque, Ciberseguridad, CSIRT, Incidente, Respuesta, Políticas.

ABSTRACT

This applied project seeks to design the main policies that provide the guidelines of action of the Center for Response to Computer Incidents of the National Open and Distance University - CSIRT-UNAD, the above, by identifying the area in which the CSIRT will act, the recognition of the guidelines and regulations related to information security that the University has defined, as well as, the consultation of good practices accepted in the world order, standards and documentation of other CSIRTs in several countries such as the United States, Spain, among others.

Some of the relevant topics addressed in the project are, the definition of security incidents, their classifications and their management, information classification, data protection, retention, destruction, disclosure and access to information, appropriate use of systems and cooperation between institutions that participate in the investigation of information security incidents.

KEYWORDS

Attack, Cybersecurity, CSIRT, incident, Response, policies.

INTRODUCCIÓN

En la actualidad, la sociedad está sumergiéndose en un nuevo 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 procesos de forma presencial, esto ha permitido ahorrar tiempo y esfuerzo, tanto así que la digitalización de la sociedad avanza a pasos agigantados.

No obstante, en la misma medida que avanza la digitalización también lo hace el cibercrimen, por lo que es necesario asegurar que la información de las personas y las empresas (para el caso, las que ofertan servicios de educación), se encuentre protegida ante cualquier evento o incidente cibernético que se pueda presentar o al cual su estructura tecnológica pueda estar expuesta.

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 que se viene desarrollando a partir del PIE denominado *“Construcción de políticas, procesos y procedimientos para la actuación administrativa del CSIRT-UNAD”*[1], tiene como propósito proporcionar los lineamientos que darán soporte administrativo a 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*

[1] ZAMBRANO HERMANDEZ, Luis, *et al*. 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” [en línea] Bogotá (Colombia) 2020 [Consultado:14 de julio de 2021]. Disponible en: https://hemeroteca.unad.edu.co/index.php/memorias/article/view/4205/4180

– *CSIRT-UNAD”*, contribuirá con el desarrollo del objetivo específico número dos del PIE, que plantea: *“Construir las políticas requeridas para la actuación administrativa del CSIRT-UNAD”*. Teniendo presente lo anterior, en este documento se presenta la construcción de las políticas principales que puede ser tomadas como referente para el funcionamiento del Centro de Respuestas a Incidentes Informáticos de la Universidad Nacional Abierta y a Distancia CSIRT-UNAD.

1. PLANTEAMIENTO DEL PROBLEMA

1.1 DEFINICIÓN DEL PROBLEMA

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 que sucedió en abril de 2016, quien fue víctima de un ataque de elevación de privilegios después de ser capturada la contraseña de varios docentes[2] y el de la Universidad del Bosque de junio de 2021 quien sufrió un ataque que afectó su página web, redes sociales, correos institucionales e información financiera[3], presentan lo inseguro que puede ser para algunas instituciones de educación superior el hacer presencia en internet.

Dado lo anterior, las universidades vienen siendo cada vez más vulnerables debido al gran almacenamiento de datos confidenciales, la poca capacidad de reacción frente a un ataque informático, la ausencia de presupuesto y de personal capacitado.[4] Un dato un poco más preocupante que presenta el Tecnológico de Monterrey, es que los ataques dirigidos a instituciones educativas de Estados Unidos, incremento un 50%, y que el foco para realizar acciones delictivas son los estudiantes.

A partir de estos datos y teniendo presente que la Universidad Nacional Abierta y a Distancia es la Universidad que presenta mayor matricula de estudiantes en más de 50 programas y que debido a su metodología, sus procesos de interacción docente-

[2] EL ESPECTADOR. [Sitio web]. Bogotá: EL ESPECTADOR. Anonymous ataca el sitio web de la Universidad de los Andes. [Consultado:14 de julio de 2021]. Disponible en: https://www.elespectador.com/actualidad/anonymous-ataca-el-sitio-web-de-la-universidad-de-los-andes-article-620617/

[3] AGENCIA DE PERIODISMO INVESTIGATIVO. [Sitio web]. Bogotá: Agencia de periodismo investigativo. Universidad del Bosque bajo ataque cibernético. [Consultado:14 de julio de 2021]. Disponible en: https://agenciapi.co/noticia/academia/universidad-del-bosque-bajo-ataque-cibernetico

[4] BRICKER & ECKLER LLP. [Sitio web]. Bricker & Eckler LLP. Privacy & Data Protection. 2015 Cybersecurity Seminar. [Consultado:14 de julio de 2021]. Disponible en: https://www.bricker.com/industries-practices/privacy-data-protection/insights-resources/resource/2015-cybersecurity-seminar-783

estudiante y estudiante administración académica, se puede desarrollar a través de sus portales virtuales y que además cuenta con estudiantes matriculados en diferentes partes del mundo, lo anterior hace que la UNAD pueda ser vista como un blanco para ciberdelincuentes puedan realizar algún tipo de acción que atente contra su Infraestructura tecnológica y por defecto impactar de forma negativa su buen nombre. Esto asociado a lo propuesto en el PIE que plantea la construcción del Centro de Respuestas a Incidentes Informáticos de la Universidad, donde se plantea el contar con equipos que puedan prevenir o remediar eventos relacionados con ciberseguridad, estos pueden ser usados para su fin, pero también al no contar con políticas que den lineamientos claros para su aplicación y uso, pueden generar situaciones que comprometan ética y legalmente al CSIRT-UNAD.

1.1.1 Pregunta problema:

Debido a la situación mencionada, el no contar con políticas claras para el desarrollo de las actividades propias del CSIRT-UNAD, puede ocasionar dificultades relacionadas con el desarrollo de las actividades propias de la Universidad y su relación con las partes interesadas, ocasionando perdidas de orden administrativo, académico y financieros.

Es así como se plantea la siguiente pregunta problema, que a partir de este documento se dará respuesta

¿Cómo el diseño de las políticas para en Centro de Respuestas a Incidentes Informáticos – CSIRT-UNAD, contribuyen en el desarrollo del proyecto de investigación denominado *“Construcción de políticas, procesos y procedimientos para la actuación administrativa del CSIRT-UNAD”* y en dar los lineamientos claros para el uso de la tecnología que soportarán los servicios brindados por este?

2. JUSTIFICACIÓN

La actuación del Centro de Respuesta a Incidentes Cibernéticos CSIRT-UNAD debe ir de la mano con la determinación de las políticas, procesos y procedimientos para la gestión de la seguridad de la información al interior de la Universidad, de tal forma que se pueda establecer las directrices y normas a seguir por el personal, permitiéndoles conocer sus roles, funciones y responsabilidades en el momento de efectuar cada una de las actividades de administración, gestión y operación propias de su quehacer en relación con los recursos existentes y los servicios ofrecidos respecto a los incidentes de ciberseguridad.

En este sentido, el presente proyecto busca apoyar la propuesta del Proyecto de Investigación de Escuela ECBTI – PIE denominado *"Propuesta para la creación y consolidación del centro de respuesta a incidentes informáticos de la Universidad Nacional Abierta y a Distancia CSIRT-UNAD"*, a través del diseño y documentación de las políticas principales que puedan proporcionar los lineamientos de actuación del Centro de Respuesta a Incidentes Informáticos de la Universidad Nacional Abierta y a Distancia: CSIRT-UNAD, considerando su articulación con las políticas vigentes de seguridad de información de la Institución.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar las políticas principales que brinden los lineamientos de actuación del Centro de Respuesta a Incidentes Informáticos de la Universidad Nacional Abierta y a Distancia – CSIRT-UNAD.

3.2 OBJETIVOS ESPECÍFICOS

Identificar el ámbito de actuación del Centro de Respuesta a Incidentes Informáticos CSIRT-UNAD, con el fin de apropiar su misión para construcción de las políticas.

Reconocer los lineamentos y normativas relacionadas con la seguridad de la información que en la actualidad la Universidad tiene definidas con el fin de articularlas con las políticas a construir.

Construir las políticas principales que permitan dar desarrollo a las actividades generadas por el Centro de Respuesta a Incidentes Informáticas del CSIRT-UNAD.

4. MARCO DE REFERENCIA

4.1. MARCO TEÓRICO

Por medio de este aspecto, se busca presentar el marco conceptual y teórico sobre el cual se va a sustentar la creación del diseño de las políticas principales que brinden los lineamientos de actuación del Centro de Respuesta a Incidentes Informáticos de la Universidad Nacional Abierta y a Distancia – CSIRT-UNAD.

4.1.1. Definición de CSIRT

Es un organismo o equipo de profesionales altamente capacitados que brinda servicios como: prevención, gestión y respuesta a incidentes de seguridad de la información a una comunidad o empresa.[5]

4.1.2. Tipos de CSIRT

Los CSIRT se pueden agrupar por sector en el cual se desempeñan, las categorías más conocidas a nivel mundial son:

CSIRT Académico: brinda sus servicios a las escuelas, universidades e institutos educativos, por lo general pueden enfocarse en investigaciones y formación estudiantil.

CSIRT Comerciales: se concentran en suplir las necesidades de las empresas respecto a la respuesta a incidentes por medio de un contrato comercial, siendo un ente externo que brinda un servicio contratado.

[5] ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. Buenas prácticas para establecer un CSIRT nacional. [Sitio web] Washington, D.C. (Estados Unidos) 2016 [Consultado:14 de julio de 2021]. Disponible en: https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2016/09/2016-Buenas-Practicas-CSIRT.pdf

CSIRT de Infraestructuras Críticas: para hablar de este tipo de CSIRT se debe tener clara la definición de infraestructura crítica: *"son todas las instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuyo proceder o destrucción el cual tendría un impacto en algunos temas como en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas".*[6]

Teniendo en cuenta lo anterior, estos CSIRT brindan sus servicios para proteger las infraestructuras críticas de un país de ataques e incidentes de seguridad de la información y pueden ser administrados por organizaciones públicas o privadas.

CSIRT Gubernamentales: se centran en proteger la infraestructura por medio de la cual el gobierno les brinda servicios a los ciudadanos.

CSIRT Nacionales: es el canal de atención y responsable de coordinación de la respuesta a incidentes a nivel nacional.

CSIRT del Sector Militar: Se encargan de la defensa de un país frente a ataques cibernéticos y están altamente capacitados para la ofensiva cibernética de ser necesario.

CSIRT de Proveedores: Pertenecen a empresas fabricantes de productos y están encargados de mitigar el impacto de las vulnerabilidades que puedan contener dichos productos.

CSIRT de empresas PYME: ayuda a las pequeñas y medianas empresas ante cualquier

[6] BERDUGO SIERRA, Helber Alirio. Importancia de definir la infraestructura critica en Colombia. [En línea]. Tesis de especialización. Universidad Militar Nueva Granada. 2016. [Consultado: 14 de julio de 2021]. Disponible en: https://repository.unimilitar.edu.co/bitstream/handle/10654/14342/BerdugoSierraHelber%20Alirio2016.pdf?sequence=1&isAllowed=y

ataque cibernético o incidente de seguridad[7].

4.1.3. Beneficios de contar con un CSIRT

- El beneficio más importante de tener un CSIRT es la capacidad de responder rápidamente ante un incidente de seguridad informática y dar respuesta de manera apropiada para mitigar el impacto de este.
- Adicionalmente, brinda otros beneficios para detectar y dar respuesta a incidentes como son:
- Proveer las herramientas necesarias para gestionar incidentes cibernéticos.
- Establecer estrategias eficientes y efectivas de alertas tempranas y respuesta.
- Comunicación con otros CSIRT de la industria que permitan establecer controles preventivos.
- Protección de los activos críticos.
- Apoyo en la concientización y capacitación de los colaboradores acerca de seguridad de la información.
- Asegurar la calidad de los sistemas desarrollados al interior de las organizaciones.
- Identificar vulnerabilidades de los sistemas que sostienen los procesos core de las organizaciones.[8]

Por otra parte, el Centro de Respuesta a Incidentes Informáticos CSIRT-UNAD tiene características de CSIRT académico, a continuación, se muestran los beneficios de contar con un CSIRT académico:

- Ser un punto de contacto en el ámbito académico para la coordinación de

[7] ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. Buenas prácticas para establecer un CSIRT nacional. [Sitio web] Washington, D.C. (Estados Unidos) 2016 [Consultado: 14 de julio de 2021]. Disponible en: https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2016/09/2016-Buenas-Practicas-CSIRT.pdf

[8] CAROZO, Eduardo; MARTINEZ, Carlos. VIDAL, Leonardo. CERTuy: Hacia un CSIRT Nacional [Sitio web] 2020 [Consultado: 14 de julio de 2021]. Disponible en: https://iie.fing.edu.uy/eventos/telcom2006/trabajos/mvdtelcom-013.pdf

respuesta a incidentes.

- Contar con infraestructura para coordinar la respuesta a incidentes protegiendo la economía de la universidad y del sector académico en el país.
- Establecer estrategias eficientes y efectivas de alertas tempranas y respuesta.
- Generar políticas con buenas prácticas para asegurar altos estándares de seguridad en la universidad.
- Comunicación con otras instituciones que gestionen incidentes cibernéticos, que permitan establecer controles preventivos mancomunados.
- Apoyo en la capacitación y concientización de la comunidad de la universidad y el sector académico acerca de seguridad de la información.[9]

4.1.4. Definición de incidente de seguridad de la información

"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".[10]

4.1.5. Clasificación de incidentes de seguridad de la Información

Incidentes de Código Dañino: hace referencia a software que busca, ingresar al sistema o dañar un equipo, servidor o dispositivo de red sin que el responsable de este lo note, por ejemplo: gusanos, spyware, troyanos, virus, ransomware, rootkit, herramientas de acceso remoto.

Incidentes de Política de Seguridad: violaciones a las directrices establecidas en las políticas de seguridad de la Compañía por parte de los usuarios ya sea por abuso de

[9] KILLCRECE, Georgia. Steps for Creating National CSIRTs. [Sitio web] Pittsburgh. 2004 [Consultado: 14 de Julio de 2021]. Disponible en: https://resources.sei.cmu.edu/asset_files/WhitePaper/2004_019_001_53064.pdf

[10] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN - ICONTEC. Ejemplo de enfoques para la categorización y clasificación de eventos e incidentes de seguridad de la información. Bogotá D.C. GTC-ISO/IEC 27035. 2015. p. 3.

privilegios, accesos a servicios no autorizados, sistemas desactualizados, entre otros.

Incidentes de Disponibilidad: son ataques dirigidos a dejar los sistemas fuera de servicio, dañar la imagen de la compañía atacada y dañar los procesos y por ende la producción por medio de denegación del servicio normal o distribuida, sabotaje, errores humanos y fallas en el software o hardware.

Incidente de Obtención de Información: son ataques que buscan obtener información más relevante para realizar ataques más avanzados como el escaneo de la red para la identificación de activos y vulnerabilidades, el sniffing, la ingeniería social y el phishing.

Incidente de Fraude: fraudes realizados por medio de la suplantación de identidad utilizando Spoofing, uso de recursos y credenciales no autorizados y/o violaciones de derechos de propiedad industrial o intelectual.

Incidentes de Intrusiones: son ataques orientados a explotar vulnerabilidades en el diseño de la configuración o funcionamiento de los sistemas con el objetivo de ingresar de forma no autorizada a los mismos, los ejemplos de este tipo de ataque son: inyección SQL, Pharming, cuenta de usuario comprometida, Cross-Site Scripting (XSS), defacement, inyección remota de ficheros, fuerza bruta, explotación de vulnerabilidades de hardware y software, y acceso no autorizado a la red.

Incidente de Compromiso de la Información: están asociados con la afectación de la confidencialidad de la información por medio del acceso no autorizado y la publicación de esta o la afectación de la integridad de está modificándola o borrándola.

Incidente de Contenido Abusivo: se asocian con el daño reputacional de la compañía utilizando sus sistemas y medios electrónicos para realizar actos ilegales como la ciberdelincuencia, acoso y publicidad con mensajes ofensivos, extorsión, violencia,

pederastia, racismo, delitos y Spam.[11]

4.1.6. Gestión de Incidentes

Hace referencia a los servicios de identificación, respuesta, mitigación y recuperación cuando ocurra un incidente de seguridad.[12]

Es recomendable para las empresas tener un esquema de gestión de incidentes para la seguridad de la información con el fin de mantener documentadas y claras las acciones a realizar cuando se presenten eventos o incidentes de seguridad[13], una de las más utilizadas es NIST con sus publicaciones SP800 y SP1800, la circular 7 de la superintendencia Financiera de Colombia está basada en ese marco y recomienda a las organizaciones que están bajo su supervisión y a las demás instituciones que quieran acogerse, que tengan en cuenta los siguientes aspectos mínimos:

Etapa de prevención: se recomienda identificar e implementar los controles que mitiguen los riesgos de ciberseguridad, incluyendo los riesgos emergentes que se den por el uso de nuevas tecnologías como IoT, inteligencia artificial, Big Data, etc., destinar un rubro para la ciberseguridad, trabajar la gestión de identidades, y asignar permisos a los usuarios únicamente a la información que necesitan, definir políticas y procedimientos.

Etapa de Protección y Detección: tener todo tipo de mecanismos para la identificación de incidentes cibernéticos, hacer pruebas de vulnerabilidades ya sea por personal interno

[11] SANCHEZ GALVÁN, Alejandro. Ciberseguridad en la industria 4.0. [En línea]. Tesis de grado. Universidad Politécnica de Valencia. 2019. [Consultado: 14 de julio de 2021]. Disponible en: https://riunet.upv.es/bitstream/handle/10251/127274/S%c3%a1nchez%20-%20Ciberseguridad%20en%20la%20industria%204.0.pdf?sequence=1&isAllowed=y
https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullReport
[12] FIRST.ORG. Foro sobre los equipos de seguridad e intervención 2 en caso de incidente 2016. p. 8 - 10.
[13] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN - ICONTEC. Ejemplo de enfoques para la categorización y clasificación de eventos e incidentes de seguridad de la información. Bogotá D.C. GTC-ISO/IEC 27035. 2015. p. 17.

o externo a la compañía y remediar las falencias evidenciadas durante las pruebas.

Etapa de Respuesta y Comunicación: Buscar la forma de ser una empresa resiliente es decir que tenga la capacidad de volver a su estado óptimo en el menor tiempo posible, para ello, se deben tener identificados claramente mecanismos de respuesta, como por ejemplo: contar con un comité de crisis capaz de decidir en cada caso si se toman medidas de erradicación de la amenaza y/o bloqueo o si se ha presentado un fraude, dar inicio a un proceso de cadena de custodia para obtener la información necesaria para que las autoridades puedan determinar acciones legales.

Etapa de Recuperación y Aprendizaje: una vez la institución se recupere del incidente presentado es necesario que realice una labor de análisis del incidente y levantamiento de lecciones aprendidas, y acciones que le permitan mejorar su ambiente de control, esas acciones deben ser implementadas y las lecciones deben ser divulgadas a las áreas involucradas con el fin de tener una retroalimentación en pro de la mejora continua.[14]

4.1.7. Tipos de servicios brindados por un CSIRT

Hay muchos servicios que puede ofrecer un CSIRT, pero generalmente están agrupados en tres categorías[15]:

Servicios reactivos: son servicios que se activan por un evento o requerimiento, como, por ejemplo, una alerta de un equipo infectado con malware o cualquier acceso no autorizado detectado por el sistema de detección de intrusos, este tipo de servicios son los más relevantes para un CSIRT.

[14] COLOMBIA. SUPERINTENDENCIA FINANCIERA DE COLOMBIA, Circular externa 007, (5, junio, 2018). Por la cual se imparte instrucciones relacionadas con los requerimientos mínimos para la gestión del riesgo de ciberseguridad. Bogotá DC. 20 p.

[15] PROYECTOAURORAONG. [Sitio web]. PROYECTOAURORAONG. Como crear un CSIRT Fundamentos. [Consultado: 14 de julio de 2021]. Disponible en: https://www.youtube.com/watch?v=2huboveQFLs

Servicios preventivos: Estos servicios ayudan a asegurar y proteger los sistemas de información por medio de la implementación de controles que mitiguen el impacto y la probabilidad de ocurrencia de incidentes de seguridad antes de que ocurran.

Servicios asociados a la gestión de calidad de la seguridad: Estos son servicios complementarios que puede brindar un CSIRT ya que están orientados a proporcionar información para ayudar a mejorar la seguridad general de las organizaciones e identificar riesgos, amenazas y debilidades del sistema, por medio de capacitaciones a los departamentos de TI de las compañías o por medio de auditorías externas que pueden contribuir indirectamente a reducir el número de incidentes.[16]

4.1.8. Clasificación de información

El objetivo de clasificar la información en un CSIRT es establecer controles suficientes para su protección según el grado de importancia que tenga en contraste con aspectos legales, de criticidad, de valor y del impacto de su divulgación o manipulación sin previa autorización,[17] es importante construir una política de clasificación de la información en el CSIRT-UNAD con criterios claros, dado que, si se dejara a percepción de las personas, la clasificación podría variar entre una y la otra.

Teniendo en cuenta lo anteriormente descrito, la complejidad de clasificación de la información varía dependiendo del ámbito del CSIRT, un ejemplo claro es el ejército, en el que existen niveles de clasificación por el rango que tenga la persona indicando así a que información se tiene acceso o los más sencillos, que cuentan con una clasificación de información sensible y no sensible, especificando el trato que se le debe dar a cada

[16] WEST-BROWN, Moira., et al. Service Categories. Handbook for Computer Security Incident Response Teams (CSIRTs). 2003. p. 24.
[17] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN - ICONTEC. Tecnología de la información. Técnicas de seguridad. Código de Práctica para controles de seguridad de la información. Bogotá D.C. GTC-ISO/IEC 27002. 2015. p. 20 - 22

una de ellas[18], no obstante, siempre se deberá velar por contar con un esquema de clasificación de la información que permita identificar aquella que realmente sea crítica.

4.1.9. Protección de datos

Un CSIRT trabaja con información sensible a la que se le debe dar un manejo apropiado por lo que es necesario contar una política que aborde el tema de protección de datos contra la divulgación y/o el tratamiento para fines no autorizados como aprovecharla para beneficio personal de los miembros del CSIRT

Al respecto, en Colombia existe la ley 1581 de 2012 de protección de datos personales que hace referencia a aspectos clave como la recolección, uso, transferencia, divulgación no autorizada, actualización, confirmación de la veracidad y eliminación de datos personales[19]

Adicionalmente, la ley colombiana 1273 de 2009 en su apartado 269f penaliza con carcel de cuarenta y ocho a noventa y seis meses e impone una multa de cien a mil salarios mínimos colombianos legales vigentes a toda persona que, sin estar autorizado, adquiera, agrupe, extraiga, ofrezca, venda, comparta, compre, divulgue, intercepte, permute, edite, emplee claves personales, ya sea que estén almacenados en carpetas, bases de datos, archivos o medios similares.[20]

4.1.10. Retención de Información

Es importante para un CSIRT contar con evidencias de los incidentes de seguridad

[18] WEST-BROWN, Moira., et al. Service Categories. Handbook for Computer Security Incident Response Teams (CSIRTs). 2003. p. 143 -144.
[19] COLOMBIA. DEPARTAMENTO NACIONAL DE PLANEACIÓN. Política nacional de explotación de datos (Big data) CONPES 3920. Por la cual se imparte instrucciones relacionadas con la explotación de datos. (17, abril, 2018). Bogotá DC. p. 19 - 21.
[20] COLOMBIA. CONGRESO DE COLOMBIA. Ley 1273. (5, enero, 2009). Por la cual se imparte instrucciones relacionadas con los delitos informáticos. Bogotá DC. p. 1 - 2.

informática salvaguardando los siguientes aspectos de estas:

Autenticidad: hay que asegurar que la información no fue modificada durante su recolección y es totalmente original.

Cadena de custodia: permite asegurar que la evidencia recolectada es confiable para respaldar un proceso judicial acusatorio de un trabajador o contratista que haya cometido un delito informático, la fiscalía general de la Nación de la República de Colombia cuenta con un manual que indica que aspectos deben tenerse en cuenta para estos casos.

Validación: se realiza con el fin de certificar que la información es la misma que se recolectó inicialmente.[21]

4.1.11. Destrucción de Información

Parte de las labores de un CSIRT es asegurar que la información confidencial que ya cumplió su ciclo de vida y no se debe utilizar más, sea borrada de tal manera que sea imposible recuperarla, para ello existen diferentes métodos de borrado de bajo nivel para discos como son:

4.1.11.1. Norma de los Estados Unidos DoD 5220-22M

Consiste en primer lugar, en escribir sobre el soporte con un valor fijo establecido, luego, con un segundo valor complementario y por último con valores aleatorios, el método consta de tres sobre escrituras y tres validaciones.

4.1.11.2 Norma de Canadá RCMP TSSIT OPS-II

[21] DELVASTO RAMÍREZ, Ramiro Andrés. Modelo de gestión de incidentes de seguridad de la información para pymes. [En línea]. Universidad nacional abierta y a distancia (UNAD). 2016 [Consultado: 14 de julio de 2021]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/6170/11324611.pdf?sequence=1&isAllowed=y

A diferencia de la anterior norma en esta se sobre escribe el disco siete veces y se hacen siete verificaciones lo que asegura que la información original del disco no pueda ser recuperable.

4.1.11.3. El estándar de la OTAN

Se sobre escribe el disco en siete veces, las seis primeras, con valores fijos diferentes entre cada sobreescritura y la última con valores aleatorios.

Datos Pseudoaleatorios:

Se usa un algoritmo llamado ISAAC, con el que se generan números de forma pseudoaleatoria y también el flujo que nombra el generados, lo más relevante de este estándar es que el usuario puede seleccionar cuantas veces quiere aplicar la sobre escritura al disco hasta un tope de 65535 veces.

4.1.11.4. Método Gutmann

Es uno de los métodos más seguros ya que a diferencia de los anteriores, se realizan las primeras cuatro pasadas de sobre escritura aleatoria sobre cada sector del disco utilizando el algoritmo ISAAC para la generación de números aleatorios, luego 27 sobre escrituras en el disco, y al final se realizan otras cuatro sobreescrituras aleatorias en cada sector del disco para un total de 35 patrones de sobreescritura.[22]

4.1.12. Divulgación de Información

[22] GARCIA PABON, Jhon Jairo. Borrado seguro de información en discos duros. [en línea]. Bogotá (Colombia). Universidad Piloto de Colombia [Consultado: 14 de julio de 2021]. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2982/00001165.pdf?sequence=1

El tiempo es muy importante a la hora de resolver incidentes, por lo que es importante construir una política de divulgación de información que le ayude al equipo de respuesta a incidentes a obtener autorización previa de parte de las partes interesadas para compartir la información asociada al mismo, a otros equipos que colaboren en la para la solución oportuna del incidente especialmente cuando es internacional, por ejemplo, la información de contacto y nombres de máquinas afectadas.[23]

Es recomendable que la política de divulgación debe contenga por lo menos los siguientes aspectos relevantes:

El proceso de divulgación de información, que puede variar dependiendo del equipo al que va dirigido y el uso que van a hacer de la información, los posibles grupos a quienes se comparte información pueden ser:

- A otros equipos cuando la aparece una nueva vulnerabilidad no identificada anteriormente o cuando están trabajando en conjunto para solucionar un incidente.
- A sitios que son el objetivo o fuente de un ataque.
- A personas que estén realizando investigaciones judiciales.
- A entidades Gubernamentales para su notificación cuando es necesario, entre otros.
- La política se debe redactar de manera general teniendo en cuenta la necesidad de conocer de las partes a quienes se les va a compartir información, adicionalmente, se debe tener en cuenta la regulación local para no ir en contra de la ley y ser sancionado.
- Por otra parte, se debe tener en cuenta la estandarización de la divulgación de la información ya que esta debe ser coherente a lo largo del tiempo, se debe definir el canal por el que va a ser publicada, enviada por correo electrónico, en un

[23] AUSCERT. [Sitio web]. Australia: AUSCERT, Forming an Incident Response Team. 2017. [Consultado: 14 de julio de 2021]. Disponible en: https://www.auscert.org.au/publications/forming-incident-response-team

repositorio al que tengan acceso los otros equipos, etc.[24]

4.1.13. Acceso a la Información

Dada la criticidad de la información contenida en los sistemas de un CSIRT, se debe establecer una política que determine quién debe acceder a la información con base a las personas que trabajan allí y los miembros de la comunidad.[25]

Inicialmente se debería identificar a que información deben tener acceso las personas con base a la premisa de que todo debe estar restringido y solo se les debe dar acceso a la información suficiente para ejecutar sus labores diarias, de la misma manera se debe definir si deben contar con permisos de lectura, escritura, borrado y/o ejecución sobre los sistemas que contienen la información, se debe incluir la utilización de contraseñas seguras utilizando caracteres especiales, letras, números, mayúsculas, signos y longitud adecuada, y se debe hacer un fuerte énfasis en la prohibición del préstamo de los usuarios de acceso a los sistemas definiendo muy bien las consecuencias de hacerlo.[26]

4.1.14. Cooperación entre equipos

Cooperar con otros equipos de respuesta ya establecidos a nivel nacional e internacional que pertenezcan al ámbito académico es fundamental ya que ayuda obtener una respuesta más contundente para detener y remediar los incidentes de seguridad, e inclusive, capturar a los responsables del ataque independiente del lugar en el que se encuentren ubicados, una forma de comunicarse con otros CSIRT es por medio de las

[24] WEST-BROWN, Moira., et al. Service Categories. Handbook for Computer Security Incident Response Teams (CSIRTs). 2003. p. 132 -135.
[25] ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. Buenas prácticas para establecer un CSIRT nacional. [Sitio web] Washington, D.C. (Estados Unidos) 2016 [Consultado:14 de julio de 2021]. Disponible en: https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2016/09/2016-Buenas-Practicas-CSIRT.pdf
[26] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN - ICONTEC. Tecnología de la información. Técnicas de seguridad. Código de Práctica para controles de seguridad de la información. Bogotá D.C. GTC-ISO/IEC 27002. 2015. p. 20 - 22

publicaciones, compartir los reportes de alertas e incidentes y brindar información propia del CSIRT con respecto a alertas y vulnerabilidades identificadas.[27]

Un ejemplo de esto es el mecanismo de coordinación que se maneja en España, en el que se establecen objetivos de colaboración para prevenir, detectar y responder ante ciberataques, para ello recomiendan establecer en las políticas, las autoridades, competencias, regulaciones y requerimientos de cada uno de los CSIRT, definir las prioridades de la gestión de las operaciones, indicar cuales son los servicios de soporte que brinda cada CSIRT, establecer protocolos de ayuda mutua, estandarizar los sistemas de gestión de emergencias, establecer objetivos y planes en común, establecer acuerdos de sistemas de alerta temprana, definir marcos de actuación en conjunto y por separado a nivel local.[28]

4.1.15. Política

Una política es un planteamiento que se da de manera general o un lineamiento que se da para que otras personas al interior de las organizaciones piensen, tomen decisiones y actúen con base en ellos.[29]

4.2. MARCO CONCEPTUAL

Los incidentes de Ciberseguridad representan un gran riesgo para una universidad que utiliza su plataforma tecnológica para bridar sus servicios a los estudiantes como es la Universidad Nacional Abierta y a Distancia UNAD, esos Ciber incidentes pueden afectar

[27] DE LA TORRE MOSCOSO, Hugo y PARRA ROSERO, Mario. Estrategia y diseño de un equipo de respuesta ante incidentes de seguridad informática (CSIRT) académico para la universidad de las fuerzas armadas ESPE. [En línea]. Universidad de las Fuerzas Armadas. 2018. [Consultado: 14 de julio de 2021]. Disponible en: http://repositorio.espe.edu.ec/bitstream/21000/15071/1/T-ESPE-040447.pdf
[28] MINISTERIO DE DEFENSA. Guía de creación de un CERT / CSIRT. España. 2011. p. 43 - 45.
[29] HIDALGO SÁNCHEZ, Narcisa. Políticas institucionalizadas por DISENSA para incrementar franquicias en el país y en la cuidad de Machala ventajas y desventajas para los franquiciados [En línea]. Tesis de grado. Universidad Técnica de Machala. 2016. [Consultado: 14 de julio de 2021]. Disponible en: http://repositorio.utmachala.edu.ec/bitstream/48000/7861/1/ECUACE-2016-AE-CD00045.pdf

de manera grave la continuidad del negocio, al respeto, es necesario generar mecanismos de respuesta que ayuden a contrarrestar esos efectos negativos, los CSIRT como equipos de respuesta a esos incidentes 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"*, deben contar con políticas que brinden los lineamientos de actuación ante los mismos.

Debido a la necesidad de establecer estrategias que permitan mejorar la seguridad de la información, la Universidad Nacional Abierta y a Distancia, desde hace varios años, viene desarrollando capacidades tecnológicas que dan respuesta a los servicios de educación ofertados, no obstante, 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.

Una manera de contribuir a dicha labor es identificando el ámbito de actuación del Centro de Respuesta a Incidentes Informáticos, con el fin de apropiar su misión para construcción de las políticas, reconociendo los lineamientos existentes con los que ya cuenta la universidad para el tratamiento y la gestión de la información y construyendo los lineamientos que debe tener el CSIRT, acerca de la clasificación de incidentes de seguridad informática, la gestión de estos en las etapas de prevención, detección, protección, comunicación, respuesta, recuperación y aprendizaje.

Otros aspectos que se deben tener en cuenta para la construcción de las políticas que contienen los lineamientos del CSIRT son: una adecuada clasificación de información, protección de datos, retención y 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.

Con base en los lineamientos establecidos, el CSIRT tendrá bases fuertes para establecer controles que le ayudarán a proteger la confidencialidad, integridad y disponibilidad de la información que administra.

4.3. MARCO LEGAL

En Colombia existen varias normas que regulan como deben ser utilizados los recursos informáticos a fin de dar buen uso a la información contenida en ellos, ya sea de empresas privadas como de personas civiles, a continuación, se menciona algunas de ellas, las cuales son relevantes para este proyecto aplicado:

4.3.1. LEY 1273 DEL 5 DE ENERO DE 2009

Esta ley aborda nueve delitos de seguridad informática y un aspecto de agravación de las condenas por motivos especiales, los nueva aspectos tienen que ver son, acceso abusivo a los sistemas informáticos, su obstaculización de manera ilegitima, la interceptación de datos informáticos, daños a los sistemas o a la información que contengan así como a sus componentes lógicos, uso de software malicioso para los ataques, violación de datos que sean denominados personales y suplantación de sitios web por medio de phishing[30].

4.3.2. LEY ESTATUTARIA 1581 DE 2012

La ley 1581 de octubre de 2012 de protección de datos personales hace referencia a aspectos clave como la recolección, uso, transferencia, divulgación no autorizada, actualización, confirmación de la veracidad y eliminación de datos personales.

4.3.3. DECRETO 1074 DE 2015

[30] COLOMBIA. CONGRESO DE COLOMBIA. Ley 1273. (5, enero, 2009). Por la cual se imparte instrucciones relacionadas con los delitos informáticos. Bogotá DC. p. 1 - 2.

Por medio de este decreto se regula la responsabilidad demostrada de los datos denominados personales, las organizaciones deben contar con un gobierno de datos el cual debe ser establecido formalmente.

4.4. MARCO ESPACIAL

Con base en lo mencionado en el planteamiento del problema y también en el objetivo del trabajo aplicado, este está enfocado en diseñar las políticas principales que brinden los lineamientos de actuación del Centro de Respuesta a Incidentes Informáticos de la Universidad Nacional Abierta y a Distancia – CSIRT-UNAD, el cual está ubicado en la capital colombiana, Bogotá D.C, en el departamento de Cundinamarca y desde allí planea brindar sus servicios utilizando las redes y telecomunicaciones de los proveedores de internet del país ISP.

Bogotá se encuentra ubicada en la parte central de Colombia, con una latitud norte: 4° 35'56'' y una longitud al oeste del meridiano de Greenwich: 74°04'51''[31], en la figura 1 se muestra el mapa de Bogotá:

Figura 1. Mapa de Bogotá

Fuente: Mapas Bogotá. Disponible en: https://mapas.bogota.gov.co/#

[31] ALCALDÍA DE BOGOTÁ. [Sitio web]. Bogotá: ALCALDÍA DE BOGOTÁ, Ubicación de la Ciudad [Consultado: 14 de julio de 2021]. Disponible en: https://bogota.gov.co/ubicacion-de-bogota-sitios-turisticos-vias-y-alrededores-de-bogota

4.5. MARCO METODOLÓGICO

4.5.1. METODOLOGÍA

Para desarrollar este proyecto, se plantea trabajara a partir de una metodología de Investigación aplicada, debido que a partir de esta se pueden encontrar estrategias que permitan aborda el problema a partir de referentes teóricos y prácticos.

La metodología será aplicada a partir de varias fases las cuales permitirán ir dando cumplimiento a los objetivos específicos propuestos:

Fase I

- Realizar la identificación del ámbito en el que actúa el CSIRT.
- Identificar la taxonomía asociada a los ataques como base para la actuación del CSIRT.
- Identificar los tipos de servicios ya sean proactivos y reactivos, junto con los servicios complementarios que el CSIRT podría ofertar.
- Identificar los perfiles del equipo de trabajo y los requisitos que son necesarios para conformar el CSIRT.

Fase II

El levantamiento de información para la creación documental se realizará por medio de indagación, análisis e investigación de fuentes documentales académicas, buenas prácticas, marcos de trabajo, estándares, documentación del CSIRT-UNAD reales, libros, videos y/o diapositivas ya sea que se encuentren de forma física o digital.

Fase III

Construcción de las políticas principales del CSIRT-UNAD, en la tabla 1 se muestra los documentos que se obtendrán como resultado:

Tabla 1. Resultados.

RESULTADO/PRODUCTO ESPERADO	INDICADOR	BENEFICIARIO
Política de clasificación de información	10%	Universidad Nacional Abierta y a Distancia – UNAD.
Política de protección de datos	20%	Universidad Nacional Abierta y a Distancia – UNAD.
Política de retención de información	30%	Universidad Nacional Abierta y a Distancia – UNAD.
Política de destrucción de información	40%	Universidad Nacional Abierta y a Distancia – UNAD.
Política de divulgación de información	50%	Universidad Nacional Abierta y a Distancia – UNAD.
Política de acceso a la información	60%	Universidad Nacional Abierta y a Distancia – UNAD.
Política de uso apropiado de los sistemas del CSIRT	70%	Universidad Nacional Abierta y a Distancia – UNAD.
Documento de Definición de Incidentes de Seguridad y Política de Eventos	80%	Universidad Nacional Abierta y a Distancia – UNAD.
Política de gestión de incidentes	90%	Universidad Nacional Abierta y a Distancia – UNAD.
Política de cooperación	95%	Universidad Nacional Abierta y a Distancia – UNAD.
Política del Cumplimiento de la Ética y la Confidencialidad	100%	Universidad Nacional Abierta y a Distancia – UNAD.

Fuente. Elaboración propia

4.5.2. MATERIALES Y RECURSOS

Los recursos y materiales que han sido utilizados para el desarrollo de este proyecto aplicado se detallan en la tabla 2:

Tabla 2. Recursos.

RECURSO	DESCRIPCIÓN	PRESUPUESTO
Equipo Humano	Andrés Vásquez Núñez	Cubierto – 0$ - Voluntariado
Equipos y Software	Computador de escritorio o mesa, Suite de Office	Cubierto – 1’500.000$

Tabla 2. (Continuación).

RECURSO	DESCRIPCIÓN	PRESUPUESTO
Viajes y Salidas de Campo	N/A	N/A – 0$
Materiales y suministros	Conexión a Internet	Cubierto – 840.000$
Bibliografía	Fuentes de información confiables que permitan sustentar el trabajo (de acceso gratuito o base de datos pagada por la universidad – Valor semestre)	Cubierto – 2´300.000$
	TOTAL	$4.640.000

Fuente. Elaboración propia

4.5.3. CRONOGRAMA

La tabla 3 muestra el tiempo que tomó desarrollar cada etapa de este trabajo:

Tabla 3. Cronograma.

ACTIVIDAD	MES 1	MES 2	MES 3	MES 4	MES 5	MES 6	MES 7	MES 8
Identificación el ámbito de actuación del CSIRT.		X						
Identificar la taxonomía asociada a los ataques como base para la actuación del CSIRT.			X	X				
Identificar los tipos de servicios ya sean proactivos y reactivos, junto con los servicios complementarios que el CSIRT podría ofertar.					X			
Identificar los perfiles del equipo de trabajo y los requisitos que son necesarios para conformar el CSIRT.					X			
Construir las políticas y procedimientos operacionales.					X	X	X	X

Fuente. Elaboración propia

5. DESARROLLO DEL PROYECTO

5.1 PANORAMA ACTUAL DE LA CIBERSEGURIDAD EN COLOMBIA

Según Mintic el total de suscriptores a internet ha venido creciendo desde los últimos años, las cifras demuestran que durante el primer trimestre del año 2017 habían 16.149.933 suscriptores, entre ellos usuarios civiles y empresas, en contraste con el primer trimestre del año 2019, en el que se contabilizaron 18.670.033 suscriptores, con una variación de crecimiento de entre el 1.19% al 2.56% trimestre tras trimestre[32], lo que demuestra que cada vez más comunidades y empresas se encuentran expuestas a los riesgos cibernéticos.

Adicionalmente, la encuesta realizada por la Organización de los Estados Americanos durante el año 2017, en el año 2016 a las empresas Colombianas, se evidenció que el 30% de las microempresas, el 40% de las pequeñas empresas, el 51% de las medianas empresas y el 63% de las grandes empresas, identificaron al menos un Ciberataque contra su organización[33], con un costo de entre 1.5 y 6 millones de pesos para microempresas, entre 10 y 20 millones de pesos para pequeñas y medianas empresas y entre 29 y 45 millones de pesos para las grandes empresas por cada ataque.

Por otra parte, el sector financiero, reportó 10.915.661 ataques cibernéticos durante el año 2016 con unas pérdidas estimadas de 6.179 millones de dólares TRM (2016).[34]
El sector académico no se queda atrás, desde hace algunos años, el sector educativo viene presentando dificultad en la gestión de la ciberseguridad respecto a su

[32] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA [Sitio web]. Bogotá: MINTIC. Total de Suscriptores de Internet a Nivel Nacional. [Consultado: 14 de julio de 2021]. Disponible en: https://colombiatic.mintic.gov.co/679/w3-propertyvalue-47275.html
[33] ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. Impacto de los incidentes de seguridad digital en Colombia. Colombia. 2017. p. 48 - 91.
[34] ASOBANCARIA. [Sitio web]. Bogotá: ASOBANCARIA, Implementación y puesta en marcha CSIRT para el sector financiero 2017. [Consultado: 14 de julio de 2021]. Disponible en: https://www.asobancaria.com/wp-content/uploads/CSIRT-Financiero-Asobancaria-julio-2018.pdf

infraestructura tecnológica, casos como el de la Universidad de los Andes la cual fue objetivo de un ataque de elevación de privilegios después de ser capturada la contraseña de varios docentes, presentan lo inseguro que puede ser para algunas instituciones de educación superior el hacer presencia en internet.

Dado lo anterior, 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 falta de personal capacitado. [35] Un dato un poco más preocupante que presente el Tecnológico de Monterrey, presenta que ataques dirigidos a instituciones educativas de Estados Unidos, incremento 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, donde Colombia se encuentra ubicada en el puesto 22 de los países más atacados de la región.[36]

Uno de los ataques recientes más significativos tuvo lugar en Colombia en el mes de octubre de 2019 según lo reportado por la empresa de seguridad ESET, donde el ataque consistió en la creación de un sitio web falso que suplantaba uno de los principales bancos del país con el fin de obtener datos de los clientes entre ellos los números y claves de tarjeta de crédito, utilizando phishing e ingeniería social para hacerlo más efectivo.[37]

[35] Bricker & Eckler LLP, (2015). Privacidad y protección de datos. Seminario de ciberseguridad 2015. [Consultado: 14 de julio de 2021]. Disponible en: https://www.bricker.com/industries-practices/privacy-data-protection/insights-resources/resource/2015-cybersecurity-seminar-783

[36] CIBERSEGURIDAD LATAM. [Sitio web]. CIBERSEGURIDAD LATAM. Kaspersky registra 45 ataques por segundo en América Latina. 2020. [Consultado: 14 de julio de 2021]. Disponible en: https://www.ciberseguridadlatam.com/2019/08/29/kaspersky-registra-45-ataques-por-segundo-en-america-latina/

[37] ESET. [Sitio web]. Welivesecurity. Falso sitio suplantaba identidad de institución financiera de Colombia para robar información de clientes. 2019. [Consultado: 14 de julio de 2021]. Disponible en: https://www.welivesecurity.com/la-es/2019/12/20/sitio-suplanta-identidad-entidad-financiera-colombia-robar-informacion-clientes/

Los expertos en seguridad de Kaspersky afirman que Colombia es uno de los países latinoamericanos que más atraen a los cibercriminales ya que cada día ocurren 28.835 ataques de phishing, atacando a bancos, proveedores de servicios, entre otros, y 566 ataques de malware a dispositivos móviles.

Con base en los resultados demostrados y los análisis realizados, se pronostica que para el año 2020 se realicen ataques dirigidos al robo de cuentas de plataformas de entretenimiento como Netflix, Spotify, Disney+ entre otras, manipulación de opinión publica a traves de redes sociales y ataques de SIM Swapping que consiste en la clonación de líneas telefónicas para hacer suplantación de identidad que permita dar acceso a los atacantes a las cuentas de las victimas aun cuando estas cuenten con factores de doble autenticación.[38]

5.2 ÁMBITO DE ACTUACIÓN DEL CSIRT.

CSIRT

En el ámbito de la ciberseguridad un CSIRT tiene como definición como: *Computer Security Incident Response Team*, para el mundo de habla hispana se definiría como Equipo de Respuesta a Incidente de Cibernéticos.

Con base en lo mencionado se puede establecer:

- Ámbitos de actuación en el que se desenvolverá el CSIRT
- El rol que tendrá el CSIRT en su ámbito de actuación.
- Actores involucrados como principales interesados en la labor que desempeñe el CSIRT.

[38] EL TIEMPO. [Sitio web]. Bogotá: EL TIEMPO. El cibercrimen no descansa, estas son las proyecciones para el 2020. [Consultado: 14 de julio de 2021]. Disponible en: https://www.eltiempo.com/tecnosfera/dispositivos/cifras-de-ciberataques-de-2019-y-tendencias-para-el-2020-435508

El Centro Criptológico Nacional de España (CCN) ha determinado en sus estudios realizados que el ámbito en el cual se desenvuelve un CERT académico es dando respuesta a los incidentes cibernéticos de las instituciones académicas ubicadas en una región, las cuales pueden ser una escuela, un instituto o una facultad.[39]

La agencia de ciberseguridad nacional de la unión europea (ENISA), con base en los estudios realizados ha determinado que un CSIRT que se desenvuelve en el sector académico es aquel que brinda servicios a las diferentes instituciones académicas y educativas como son las universidades o los centros de investigación y sus plataformas web implementadas para dar respuesta a la necesidad de los estudiantes de estudiar de manera no presencial o campus virtuales.[40]

De acuerdo a lo anteriormente expuesto, con el objetivo de alcanzar la meta establecida por la Universidad Nacional Abierta y A Distancia - UNAD en el plan de desarrollo de los años 2019 al 2023, donde se planteó que se desarrollarían proyectos y estrategias que contaran con un carácter de tipo científico tecnológico y de innovación, que permitan el fortalecimiento del sector productivo y el sector educativo de Colombia, adicionalmente se propuso que durante el año 2021 se implementaría el SOC (Sistema Operación de seguridad informática)[41]

El ámbito de actuación propuesto es el de la consolidación de un Centro de Respuesta a Incidentes Cibernéticos de la Universidad Nacional Abierta y a Distancia, este gira en torno a lo académico y tiene como meta brindar respuesta a los incidentes cibernéticos que afecten a las comunidades académicas como las universidades, instituciones educativas y colegios con base en su tamaño e instalaciones y focalizando sus esfuerzos en promover espacios de I+D+I.

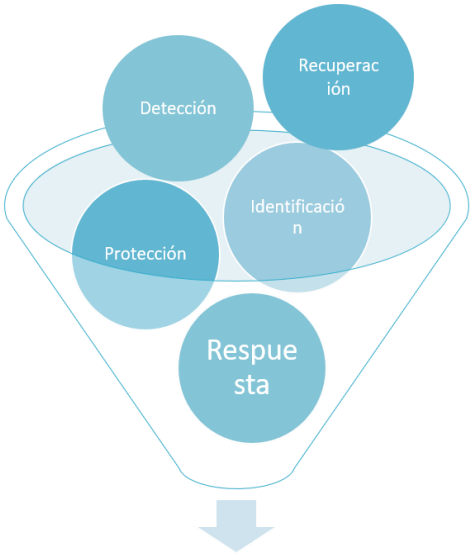
[39] MINISTERIO DE DEFENSA. Guía de creación de un CERT / CSIRT. España. 2011. p. 43 - 45.
[40] ENINSA. Cómo crear un CSIRT paso a paso. Colombia. 2006. p. 21 - 25
[41] UNIVERSIDAD NACIONAL ABIERNA Y A DISTANCIA UNAD. Plan de desarrollo 2019 – 2023. Bogotá D.C. 2018. 118 p.

5.2.1 Ámbito de Actuación del CSIRT-UNAD

El ámbito de actuación propuesto para el Centro de Respuesta a Incidentes de la Universidad Nacional Abierta y a Distancia - UNAD es el académico, el cual tiene como fin: apoyar en la reacción ante eventos o incidentes cibernéticos para reducir su impacto en comunidades académicas, adicionalmente generará documentación que ayuden a la prevención y alertamiento de la comunidad objetivo.

La figura 2 muestra el esquema del CSIRT de la Universidad Nacional Abierta y a Distancia.

Figura 1. Esquema de CSIRT Académico, CSIRT-UNAD.



Equipo que brinda apoyo para la reacción ante eventos o incidentes cibernético con el fin de reducir su impacto. Tiene además como función la generación de documentos que prevengan y alerten a la comunidad objetivo

Fuente: ZAMBRANO HERMANDEZ, Luis, et al. 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" [en línea]. Bogotá (Colombia) 2020 [Consultado:14 de julio de 2021]. Disponible en: https://hemeroteca.unad.edu.co/index.php/memorias/article/view/4205/4180

5.2.2 Papel del CSIRT-UNAD

El rol que desempeña el CSIRT-UNAD, es ser el primer Centro de Respuestas a Incidentes Informáticos Académico de Colombia, persiguiendo el objetivo de impactar en, institutos de educación superior, Universidades, institutos de educación para el desarrollo humano, Colegios públicos y privados para brindar soluciones a problemas asociados a la Ciberseguridad.

5.2.3 Partes Interesadas

El principal sector impactado con el CSIRT – UNAD es el académico, no obstante, existen otras partes interesadas de los servicios de este como son el sector económico colombiano al cual se le puede realizar acompañamiento, las pequeñas, medianas y grandes empresas e infraestructura critica del país pueden ser otras partes que se pueden ver beneficiadas por los servicios del CSIRT – UNAD.

En la tabla 4 se presenta el actual estado de Colombia en materia de Ciberseguridad comparándola con Latinoamérica utilizando la metodología semaforizada.

Tabla 4. Estado actual de Colombia en términos de Ciberseguridad respecto a Latinoamérica.

Medidas Legales		Medidas Técnicas		Medidas Organizacionales		Capacidad de Creación		Cooperación	
LAT	**COL**	**LAT**	**COL**	**LAT**	**COL**	**LAT**	**COL**	**LAT**	**COL**
Legislación Cibercriminal		CERT/CIRT/CSIRT Nacionales		Estrategia		Cuerpos estandarizados		Acuerdos bilaterales	
Legislación en Ciberseguridad		CERT/CIRT/CSIRT de Gobierno		Agencias responsables		Buenas prácticas en ciberseguridad		Acuerdos multilaterales	
Entrenamiento en Seguridad		CERT/CIRT/CSIRT Sectorial		Métricas de Ciberseguridad		Programas de I+D+i		Participación internacional	

Tabla 4. (Continuación).

Medidas Legales		Medidas Técnicas		Medidas Organizacionales		Capacidad de Creación		Cooperación	
LAT	**COL**	**LAT**	**COL**	**LAT**	**COL**	**LAT**	**COL**	**LAT**	**COL**
		Estándar para Organizaciones				Campaña de concientización publicas		Asociaciones público-privadas	
		Estándar para profesionales				Cursos de entrenamiento profesional		Asociaciones inter-agencias	
		Protección en Línea para Menores				Programas educativos			
						Mecanismos de incentivos			
						Industrias de ciberseguridad propias			

Fuente: ZAMBRANO HERMANDEZ, Luis, et al. 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" [en línea] Bogotá (Colombia) 2020 [Consultado:14 de julio de 2021]. Disponible en: https://hemeroteca.unad.edu.co/index.php/memorias/article/view/4205/4180.

LAT = Latinoamérica

COL = Colombia

En conclusión, se relacionan posibles partes interesadas

- Sector académico
- Microempresa
- Infraestructuras Criticas
- Grandes Empresas
- Pequeñas y Medianas Empresas

5.3 TAXONOMÍA DE ATAQUES RELEVANTES

A continuación, se define la clasificación de incidentes que son relevantes para el CSIRT-UNAD, teniendo en cuenta el panorama de ciberseguridad de Colombia.

Incidente de Obtención de Información: son ataques que buscan obtener información más relevante para realizar ataques más avanzados como el escaneo de la red para la identificación de activos y vulnerabilidades, el sniffing, la ingeniería social y el phishing.

Incidentes de Código Dañino: hace referencia a software que tiene como objetivo, ingresar al sistema o dañar un equipo, servidor o dispositivo de red sin que el responsable de este lo note, por ejemplo: virus, gusanos, troyanos, spyware, rootkit, ransomware, herramientas de acceso remoto.

Incidentes de Política de Seguridad: violaciones a las directrices establecidas en las políticas de seguridad de la empresa por parte de los usuarios ya sea por abuso de privilegios, accesos a servicios no autorizados, sistemas desactualizados, entre otros.

Incidentes de Disponibilidad: son ataques dirigidos a dejar fuera de servicio los sistemas, dañar la imagen de la compañía atacada y/o dañar los procesos y por ende la producción por medio de denegación del servicio normal o distribuida, sabotaje, errores humanos y fallas en el software o hardware.

Incidente de Fraude: fraudes realizados por medio de la suplantación de identidad utilizando Spoofing, uso de recursos y credenciales no autorizados y/o violaciones de derechos de propiedad industrial o intelectual.

Incidentes de Intrusiones: son ataques orientados a la explotación de vulnerabilidades en el diseño de la configuración o funcionamiento de los sistemas con el objetivo de ingresar de forma no autorizada a los mismos, los ejemplos de este tipo de ataque son: inyección SQL, Pharming, compromiso de cuenta de usuario, defacement, Cross-Site Scripting (XSS), ataque de fuerza bruta, inyección de ficheros remota, explotación de

vulnerabilidades de software y hardware, y acceso no autorizado a la red.

Incidente de Compromiso de la Información: están relacionados con la afectación de la confidencialidad de la información por medio del acceso no autorizado y la publicación de esta o la afectación de la integridad de está, modificándola o borrándola.

Incidente de Contenido Abusivo: están orientados en dañar la imagen de las compañías utilizando sus sistemas y medios electrónicos para usos ilegales como la ciberdelincuencia, acoso, extorsión y publicidad con mensajes ofensivos, violencia, pederastia, racismo, delitos y Spam.[42]

5.4. CATÁLOGO DE SERVICIOS DEL CSIRT

Los servicios brindados por el CSIRT-UNAD están categorizados en tres frentes que son servicios proactivos, reactivos y complementarios:

5.4.1. Servicios Proactivos

Estos servicios están enfocados en brindar asistencia e informar a la Universidad Nacional Abierta y a Distancia, ayudarla a prepararse para proteger y asegurar los sistemas, anticipando problemas, ataques y/o eventos, con el fin de reducir significativamente la cantidad de incidentes que se puedan presentar en el futuro.

- Anuncios de seguridad de la información de buenas prácticas que ayudarán al ambiente de control de las organizaciones.
- Auditorías de seguridad a la plataforma tecnológica.

[42] SANCHEZ GALVÁN, Alejandro. Ciberseguridad en la industria 4.0. [En línea]. Tesis de grado. Universidad Politécnica de Valencia. 2019. [Consultado: 14 de julio de 2021]. Disponible en: https://riunet.upv.es/bitstream/handle/10251/127274/S%c3%a1nchez%20-%20Ciberseguridad%20en%20la%20industria%204.0.pdf?sequence=1&isAllowed=y
https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullReport

- Test de intrusión para detección de vulnerabilidades.
- Divulgación de información de seguridad comunicando fallas identificadas por el sector y su remediación.

5.4.2. Servicios Reactivos

Se ponen en marcha ante un evento, petición o incidente de seguridad ocurrido, que por lo general pueden ser identificados por un sistema IDS o de detección de intrusos o un sistema SIEM de registro de eventos.

- Alertas y advertencias de detección de ataques informáticos de acuerdo con el monitoreo realizado.
- Gestión, análisis y respuesta a incidentes de ciberseguridad presentados.
- Monitorización del portal web.
- Detección de intrusiones.

5.4.3. Servicios Complementarios

Estos servicios ayudan a mejorar el ambiente de control de seguridad de la información de la universidad y consiste en compartir el conocimiento y experiencia que tiene el CSIRT con el fin de generar conciencia en el recurso humano, se ve reflejado en:

- Formación a los colaboradores de la universidad.
- Concienciación por medio de campañas.
- Asesoría técnica donde se solucionen inquietudes específicas sobre configuraciones de seguridad en los dispositivos de red, e infraestructura de la organización.
- Asesoría legal en materia de seguridad.

5.5. ORGANIZACIÓN Y TALENTO HUMANO

5.5.1. Perfiles de cargo que requiere el CSIRT-UNAD.

En la tabla 3 se muestra la estructura organizacional propuesta para el Centro de Respuestas a Incidentes Cibernéticos CSIRT-UNAD:

Figura 3: Estructura Organizacional del CSIRT-UNAD.

Fuente: ZAMBRANO HERMANDEZ, Luis, et al. 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" [en línea] Bogotá (Colombia) 2020 [Consultado:14 de julio de 2021]. Disponible en: https://hemeroteca.unad.edu.co/index.php/memorias/article/view/4205/4180.

En la tabla 5 se muestra los perfiles administrativos, operativos y de apoyo que requiere el CSIRT – UNAD:

Tabla 5: Relación de los perfiles que requiere el CSIRT-UNAD para su buen funcionamiento.

Orden	Perfil
Directivo	Director
Administrativo	Gestor de Comunicaciones
	Asesor Jurídico
	Consultor Externo
Operativo y de Apoyo	Coordinador CSIRT-UNAD
	Gestor Investigador
	Gestor de Mitigaciones
	Gestor Post-Incidente
	Gestor de Diagnostico o Triage
	Gestor de Red y de Sistemas de Información
	Operador del CSIRT-UNAD

Fuente: ZAMBRANO HERMANDEZ, Luis, et al. 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" [en línea] Bogotá (Colombia) 2020 [Consultado:14 de julio de 2021]. Disponible en: https://hemeroteca.unad.edu.co/index.php/memorias/article/view/4205/4180.

5.5.2. Funciones y Responsabilidades

A continuación, se hace una relación de aquellas funciones y responsabilidades asociadas a los perfiles de cargo que se requieren para ejecutar los servicios que han sido propuestos para el Centro de Respuestas a Incidentes Cibernéticos CSIRT-UNAD, por un lado, para los perfiles directivos y administrativos en la tabla 6, por otro lado, para los perfiles operativos y de apoyo logístico en la tabla 7.

La estructura con la que se aborda cada perfil es: objetivo del perfil, responsabilidades, las actividades asociadas al cargo, experiencia requerida para el cago, habilidades necesarias para la ejecución de las labores asociadas al cargo.

Tabla 6. Perfiles directivos y administrativos del CSIRT-UNAD.

Perfil	Función
Director	● Direccionar de forma estratégica al CSIRT-UNAD. ● Entrevistar y contratar a nuevos colaboradores del CSIRT-UNAD. ● Asistir a reuniones del consejo asesor de seguridad o algún otro que requiera la estructura orgánica de la Universidad. ● Representar al CSIRT en los eventos.
Gestor de Comunicaciones	● Desarrollar y publicar artículos o documentos que se relacionen con el CSIRT-UNAD y mantener actualizados a los medios con información del CSIRT-UNAD ● Representar al CSIRT-UNAD ante los medios de comunicación con la autorización previa de la Dirección. ● Realizar las redacciones necesarias para alertar a la comunidad académica y generar boletines
Asesor Jurídico	● Acompañar y asesorar los procesos jurídicos que se relaciones con los servicios brindados por el CSIRT-UNAD. ● Supervisar y apoyar los procesos legales de conformación del CSIRT-UNAD y las vinculaciones de afiliados.
Consultor Externo	● De acuerdo con la necesidad del servicio, se realizará requerimiento.

Tabla 6. (Continuación).

Perfil	Función
Coordinador CSIRT-UNAD	● Apoyar los procesos de la Dirección. ● Supervisar la operación del equipo de trabajo. ● Liderar al equipo en las labores diarias designando deberes y tareas al mismo. ● Autorizar el acceso a la información a partir de la necesidad de conocerla. ● Salvaguardar la información clasificada como confidencial. ● Si así se requiere, capacitar a otros miembros del equipo del CSIRT-UNAD.

Fuente: ZAMBRANO HERMANDEZ, Luis, et al. 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" [Sitio web] Bogotá (Colombia) 2020 [Consultado:14 de julio de 2021]. Disponible en: https://hemeroteca.unad.edu.co/index.php/memorias/article/view/4205/4180

Tabla 1: Perfiles operativos y de apoyo logístico del CSIRT-UNAD.

Perfil	Función
Gestor de Diagnóstico o Triage	● Clasificar y priorizar incidentes y eventos. ● Asignar los casos presentados al técnico adecuado. ● Analizar incidentes, monitorear, registrar y escalar el incidente o evento al técnico correspondiente
Gestor Investigador	● Investigar los casos puntuales que se presenten. ● Desarrollar material técnico para capacitar al equipo del CSIRT-UNAD. ● Realizar tareas de monitoreo para la investigación. ● Desarrollar herramientas para obtención de datos estadísticos y métricas. ● Transferir conocimiento a los miembros del equipo del CSIRT-UNAD

Tabla 2: (Continuación).

Perfil	Función
Gestor de Mitigación	● Analizar incidentes, monitorear, registrar y dar oportuna respuesta ante incidentes y eventos. ● Coordinar la respuesta a incidentes y presentar informes al coordinador del CSIRT-UNAD. ● Interactuar con otros grupos de respuesta a incidentes o técnicos para resolver los eventos presentados.
Gestor Post-Incidente	● Brindar asistencia inicial de respuesta a los Incidentes. ● Clasificar y priorizar la información asociada a los eventos presentados. ● Generar documentos con las lecciones aprendidas que se puedan utilizar como base de conocimiento.
Gestor de Red y de Sistemas de Información	● Gestionar y dar respuesta a los incidentes asociados con la red y los sistemas del CSIRT-UNAD. ● Administrar y mantener los sistemas de información y la infraestructura del CSIRT-UNAD. ● Asistir y responder a los incidentes, cuando estos así lo requieran. ● Gestionar los accesos a la información a los integrantes del CSIRT- UNAD.
Operador de CSIRT-UNAD	● Analizar, ejecutar, gestionar y dar cumplimiento a las actividades que se le asignen. ● Reportar los incidentes de seguridad. ● Actualizar la base de conocimientos. ● Dar soporte y solucionar de oportunamente los incidentes y problemas reportados con base en los SLA´s. ● Asegurar los casos escalados cuenten con toda la información necesaria. ● Asegurar la calidad y profesionalismo al ejecutar las actividades del día a día. ● Hacer seguimiento a los casos abiertos.

Tabla 3: (Continuación).

Perfil	Función
Operador de CSIRT-UNAD	● Monitorear el estado de los sistemas y la red con herramientas SIEM, identificando posibles amenazas en la red de los clientes.

Fuente: ZAMBRANO HERMANDEZ, Luis, et al. 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" [en línea] Bogotá (Colombia) 2020 [Consultado:14 de julio de 2021]. Disponible en: https://hemeroteca.unad.edu.co/index.php/memorias/article/view/4205/4180.

5.6. LINEAMENTOS Y NORMATIVAS RELACIONADAS CON LA SEGURIDAD DE LA INFORMACIÓN DEFINIDAS POR LA UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD.

Al realizar una consulta documental de los lineamientos existentes en la Universidad Nacional Abierta y a Distancia – UNAD, se identificó que la misma cuenta con diferentes resoluciones que sirven como base para la definición de las políticas, las cuales son:

Resolución 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"*.[43]

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"*[44]

[43] UNIVERSIDAD NACIONAL ABIERTA Y ADISTANCIA UNAD. Resolución No. 2945. Bogotá D.C.: Universidad Nacional Abierta y a Distancia, 2009. 4 p.
[44] UNIVERSIDAD NACIONAL ABIERTA Y ADISTANCIA UNAD. Resolución No. 2943. Bogotá D.C.: Universidad Nacional Abierta y a Distancia, 2009. 3 p.

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"*.[45]

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)"*.[46]

Resolución 5071: *"Por la cual se define la política de renovación tecnológica de la Universidad Nacional Abierta y a Distancia – UNAD"*.[47]

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"*.[48]

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"*.[49]

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"*.[50]

---

[45] UNIVERSIDAD NACIONAL ABIERTA Y ADISTANCIA UNAD. Resolución No. 2944. Bogotá D.C.: Universidad Nacional Abierta y a Distancia, 2009. 7 p.
[46] UNIVERSIDAD NACIONAL ABIERTA Y ADISTANCIA UNAD. Resolución No. 6018. Bogotá D.C.: Universidad Nacional Abierta y a Distancia, 2012. 6 p.
[47] UNIVERSIDAD NACIONAL ABIERTA Y ADISTANCIA UNAD. Resolución No. 5071. Bogotá D.C.: Universidad Nacional Abierta y a Distancia, 2013. 15 p.
[48] UNIVERSIDAD NACIONAL ABIERTA Y ADISTANCIA UNAD. Resolución No. 2110. Bogotá D.C.: Universidad Nacional Abierta y a Distancia, 2008. 15 p.
[49] UNIVERSIDAD NACIONAL ABIERTA Y ADISTANCIA UNAD. Resolución No. 0190. Bogotá D.C.: Universidad Nacional Abierta y a Distancia, 2010. 4 p.
[50] UNIVERSIDAD NACIONAL ABIERTA Y ADISTANCIA UNAD. Resolución No. 156. Bogotá D.C.: Universidad Nacional Abierta y a Distancia, 2013. 5 p.

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"*.[51]

Resolución 5303: *"Por el cual se expide el código de ética y de buen gobierno de la UNAD"*.[52]

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"*.[53]

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"*.[54]

Al respecto, se puede identificar que las mismas se encuentran vigentes y pueden complementar las políticas propuestas para el desarrollo de las actividades generadas por el CSIRT UNAD, esta relación se muestra en la tabla 8:

Tabla 8. Resoluciones que podrían tomarse como base para la documentación de políticas principales del CSIRT – UNAD.

Resolución	Aspecto abordado por la resolución	Política que tendría como base la resolución existente.
Resolución 2945	Uso de los servicios de tecnología informática y telecomunicaciones de la UNAD.	Política de Uso Apropiado de los Sistemas del CSIRT.

[51] UNIVERSIDAD NACIONAL ABIERTA Y ADISTANCIA UNAD. Resolución No. 4793. Bogotá D.C.: Universidad Nacional Abierta y a Distancia, 2013. 18 p.
[52] UNIVERSIDAD NACIONAL ABIERTA Y ADISTANCIA UNAD. Resolución No. 5303. Bogotá D.C.: Universidad Nacional Abierta y a Distancia, 2008. 9 p.
[53] UNIVERSIDAD NACIONAL ABIERTA Y ADISTANCIA UNAD. Resolución No. 6858. Bogotá D.C.: Universidad Nacional Abierta y a Distancia, 2014. 5 p.
[54] UNIVERSIDAD NACIONAL ABIERTA Y ADISTANCIA UNAD. Resolución No. 7966. Bogotá D.C.: Universidad Nacional Abierta y a Distancia, 2014. 4 p.

Tabla 8. (Continuación).

Resolución	Aspecto abordado por la resolución	Política que tendría como base la resolución existente.
Resolución 2943	Clasificación y el manejo de la información confidencial en la UNAD.	Política de Clasificación de Información.
Resolución 2944	Seguridad informática y el uso adecuado de la tecnología para el procesamiento de la información en la UNAD.	Política de Uso Apropiado de los Sistemas del CSIRT.
Resolución 6018	Clasificación y el manejo de la información confidencial en la UNAD.	Política de Clasificación de Información.
Resolución 5071	Renovación tecnológica de la UNAD.	Política de Uso Apropiado de los Sistemas del CSIRT.
Resolución 2110	Creación del Sistema de Gestión Tecnológica –SIGETEC, de la UNAD, y conformación el Comité Estratégico del Sistema de Gestión Tecnológica y la Mesa Técnica para su operación.	Política de gestión de incidentes.
Resolución 0190	Conformación del Grupo Funcional de Gestión Técnica de la Plataforma Tecnológica Integrada, de la UNAD.	Política de gestión de incidentes.
Resolución 156	Actualización del sistema de gestión documental de la UNAD.	Política de Retención de Información.
Resolución 4793	Seguridad de la Información y Gestión Documental de la UNAD.	Política de Retención de Información

Tabla 8. (Continuación).

Resolución	Aspecto abordado por la resolución	Política que tendría como base la resolución existente.
Resolución 5303	Código de ética y de buen gobierno de la UNAD	Política del Cumplimiento de la Ética y la Confidencialidad
Resolución 6858	Comité técnico de gestión integral y MECI	Política de Retención de Información.
Resolución 7966	Se conforma el SIG - UNAD, se establece la política integrada de gestión	Política de Retención de Información.

Fuente. Elaboración propia.

5.7. MANUAL DE POLÍTICAS PRINCIPALES PARA EL DESARROLLO DE LAS ACTIVIDADES GENERADAS POR EL CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICAS DEL CSIRT-UNAD.

5.7.1. Política de clasificación de información

Objetivo: Establecer 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-UNAD, 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.

Alcance: Todo activo de información perteneciente al CSIRT - UNAD y sus clientes, que se encuentre en poder de la organización o proveedores y externos autorizados para administrarlos.

Definiciones:

Activo de Información: información que tenga valor y sea de importancia para el CSIRT - UNAD, relevante, entre otras, en el almacenamiento, comunicación, producción y emisión, la cual puede fluir en diversos medios que hay que resguardar para que cumplan su propósito:

- Medios circulables físico y digital, en todos los formatos (papel impreso, archivos digitales, audio, imagen, video).
- La infraestructura, sistemas, equipos que soportan esa información.
- Las personas que hacen uso de la información, y que conocen los procesos institucionales. [55]

Incidente de Seguridad: Cualquier situación que exponga a un riesgo, entre otros, la confidencialidad, disponibilidad o integridad propia de la información. Son ejemplos de lo anterior, el robo de un computador, el incumplimiento de un reglamento de seguridad, infección de un virus, correos sospechosos, caída de un sistema, etc. [56]

Dispositivo tecnológico: Cualquier equipamiento computacional de uso personal o para fines del trabajo: Notebook, tablet, desktop, smartphone u otro similar, propio o de propiedad de la empresa que contenga información de CSIRT - UNAD, como correos, grupos de trabajo, archivos o acceso a aplicativos.

Dispositivo de almacenamiento: Cualquier elemento portable que permita almacenar información digital (notebook, teléfono, memoria USB, etc.)

[55] CAVIEDES SANABRIA, Fernando y PRADO URREGO, Bertulfo. Modelo unificado para identificación y valoración de los riesgos de los activos de información en una organización. [En línea]. Universidad ICESI. 2012. [Consultado: 14 de julio de 2021]. Disponible en: https://pdfs.semanticscholar.org/c8a0/cc6a02ce0b801df4442a32e1bc8e67f20cc2.pdf

[56] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN - ICONTEC. Ejemplo de enfoques para la categorización y clasificación de eventos e incidentes de seguridad de la información. Bogotá D.C. GTC-ISO/IEC 27035. 2015. p. 3.

Custodio de la Información: Colaborador encargado de generar procedimientos y planes de acción requeridos para resguardar la información que transita en el proceso.

Colaborador: Toda persona que pertenezca a la nómina de personal interno del CSIRT - UNAD y tenga un vínculo contractual de trabajo con el CSIRT - UNAD.

Aspectos Generales:

Actividades asociadas a la clasificación de los activos de información:

Identificación de Activos de Información

El CSIRT - UNAD debe impulsar la detección y tratamiento de sus activos de información, documentarlos y clasificarlos en un inventario de activos.

Velar por la identificación y clasificación de los activos de información es una responsabilidad que cada dueño de los datos, el cual debe gestionar que se denomine un custodio de esta información.

Identificar Propietario de los Activos de Información

Cada uno de los activos de información inventariados debe poseer un propietario, quien poseerá mayor injerencia sobre estos, para asegurar su tratamiento adecuado, y a su vez, se debe designar a un responsable que lleve a cabo la actividad de *"custodio"*, monitoreando sus avances.

El Custodio designado, generará procedimientos y planes de acción requeridos para el resguardo de los activos de información.

Clasificación de la Información

La información tiene distintos grados de criticidad y sensibilidad, de modo que se clasifica en términos de su valor y riesgos. La clasificación adoptada, debe permitir conocer la necesidad, las prioridades y el grado de protección esperado en el manejo de la información.

Se considera un *"Activo Crítico de Información"* a cualquiera que tenga una de las categorías en su nivel más alto.

En tal sentido, en la tabla 9 se distinguen las categorías de clasificación de los activos de información:

Tabla 9. Categorías para la clasificación de activos de información.

CONFIDENCIALIDAD	**DISPONIBILIDAD**	**INTEGRIDAD**
Confidencial y Privado: Información que únicamente debe conocer y utilizar un grupo muy reducido de colaboradores del CSIRT - UNAD, la cual, si se divulga o se usa de manera no autorizada, puede materializar riesgos o pérdidas graves a la organización o a terceros. Dispuesta para algunas entidades externas solamente si está autorizada por la Dirección del CSIRT.	**Alta:** Más de 1 hora sin disponer de esta información, podría ocasionar riesgos o pérdidas graves a la organización o a terceros.	**Alta:** Toda información reportada a entidades fiscales, información financiera y para decisiones comerciales. Tener errores en esta información, podría ocasionar riesgos o pérdidas muy graves a la organización o a terceros.

Tabla 9. (Continuación).

CONFIDENCIALIDAD	DISPONIBILIDAD	INTEGRIDAD
Uso Interno: Información que sólo puede ser conocida y utilizada al interior del CSIRT - UNAD. Compartirla con externos sólo con autorización del subgerente o jefe directo.	**Media:** Más de 1 semana sin disponer de esta información, podría ocasionar riesgos o pérdidas considerables a la organización.	**Baja:** Se asume que debe ser Integral, pero no es la principal característica.
Pública: La información no cuenta con restricciones para ser conocida y usada por parte de cualquier persona, sin necesidad de autorización, sea colaborador o no.	**Baja:** Puede ser recuperado en más de una semana, sin generar daños considerables.	

Fuente. Elaboración propia.

Responsabilidades:

Personal del CSIRT: todos los colaboradores que hagan parte del CSIRT, independientemente de su cargo deben manejar de manera adecuada los datos a los cuales tiene acceso.

Propietario del activo: persona responsable de clasificar y etiquetar los activos de información, en lo posible será el jefe del área.

Administrador de los Sistemas: es el encargado de documentar los activos en el inventario, con base en la clasificación que tendrán, adicionalmente, será quien configure los permisos de acceso en los diferentes sistemas del CSIRT a quien se de autorización por parte del propietario de los datos.

5.7.2. Política de protección de datos

Objetivo: Definir 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.

Alcance: Esta política aplica para cualquier registro de datos personales de clientes, usuarios, proveedores y empleados recolectada por el CSIRT presencialmente, no presencial y/o por medios virtuales con el fin de vincularlos a los servicios brindados por el CSIRT.

Definiciones:

Autorización: Consentimiento informado del titular de los datos personales con el fin de poder utilizarlos según lo que se informa de manera anticipada al mismo.

Dato semiprivado: Hace referencia al dato que no es reservado, público, ni íntimo, y que al ser divulgado o conocido puede interesar tanto al titular, como a un grupo específico de personas e inclusive a toda la sociedad.

Dato público: Dato que puede ser conocido y utilizado por parte de cualquier persona, sin necesidad de autorización, sea colaborador o no.

Dato personal: Cualquier dato que se pueda asociar con una o más personas.

Dato sensible: Dato que está directamente ligado a la intimidad de una persona el cual puede causar discriminación si se utiliza de manera indebida, algunos de ellos son: inclinación política, origen racial, origen étnico, creencias religiosas y/o filosóficas, datos biométricos, vida sexual, Etc.

Encargado del tratamiento: Persona jurídica, privada, pública o natural, que por sí misma o asociada con otros, trata los datos personales en vez del encargado del tratamiento.

Responsable del tratamiento: Persona jurídica, privada, pública o natural, que sola o asociada con otros, tiene poder de decidir acerca de la base de datos y su tratamiento.

Tratamiento: Acción realizada sobre datos personales, como recolectarla, almacenarla, usarla o suprimirla[57]

Titular: se trata de la persona denominada natural de quien se reciben datos para ser tratados.

Aspectos Generales:

Circulación restringida y acceso: Los datos que son denominados personales, menos aquella información que se considera pública tiene restricción y no se podrán publicar en internet, ni en ningún otro medio de comunicación masiva, a no ser que se pueda controlar técnicamente para otorgar un acceso únicamente a las personas titulares o a los terceros autorizados por ellos, a dichos datos.

Transparencia: Al capturar, usar y tratar los datos personales, se debe garantizar el derecho de la persona a quien pertenecen los datos, de obtener por parte del CSIRT -

[57] COLOMBIA. SENADO DE LA REPÚBLICA. Ley 1581. (17, octubre, 2012) protección de datos personales. Por la cual se imparte instrucciones relacionadas con la explotación de datos. Bogotá. p. 68.

UNAD, en cualquier momento y sin ninguna restricción, información sobre la existencia de cualquier dato considerado personal.

Calidad o veracidad: La información capturada, que sea recolectada, utilizada y tratada debe estar completa, ser exacta, veraz, estar actualizada, ser comprensible y comprobable. Se prohíbe tratar datos que estén incompletos, que sean parciales, que estén fraccionados o que puedan inducir a error.

Finalidad: La recolección y tratamiento de datos personales realizados por el CSIRT – UNAD, atenderán una finalidad legítima y estarán subordinados, dicha finalidad deberá informarse a la persona titular de los datos.

Libertad: Capturar y tratar los datos personales únicamente se podrá realizar con el consentimiento anticipado de la persona titular, adicional a ello, no se podrán obtener ni divulgar datos personales sin autorización anticipada, sin un mandato judicial, estatutario o legal que demuestre que se cuenta con el consentimiento.

Legalidad: Al capturar, recolectar y tratar los datos personales, se aplicará lo establecido en la ley colombiana vigente que reglamente el tratamiento de los datos personales.

Seguridad: CSIRT - UNAD cuenta con profesionales dedicados a la seguridad de la información los cuales velarán por mantener la integridad, confidencialidad y disponibilidad de los datos que el CSIRT tiene a su cargo.

Para esto utilizarán procedimiento de novedades de usuarios, políticas de control de acceso configuradas en el firewall, para brindar acceso a dichas bases de datos, se debe contar con autorización previa de los propietarios de la información y finalmente, se incluye el monitoreo sobre la actividad de usuarios finales, encargados y administradores, sobre dichas bases de datos.

Se gestionarán las vulnerabilidades de los sistemas que contienen las bases de datos y se aplicará cifrado a las mismas.

Confidencialidad: El CSIRT - UNAD exigirá a sus colaboradores que tengan acceso a información contenida en sus bases de datos, que firmen un acuerdo de confidencialidad en el que se comprometen a no divulgar y/o utilizar la información para obtener beneficio propio o de terceros, sino por el contrario, a mantener la confidencialidad de esta.[58]

Responsabilidades:

El CSIRT - UNAD con base en la normatividad actual, será quien rendirá cuentas del tratamiento de datos personales realizado.

5.7.3. Política de retención de información

Objetivo: Definir el tiempo en que se retendrá los datos recolectados por el CSIRT – UNAD de acuerdo con su clasificación.

Alcance: Todos los colaboradores de CSIRT – UNAD deberán acogerse a estos lineamientos de retención de información.

Definiciones:

Es importante para un CSIRT contar con evidencias de los incidentes de seguridad informática salvaguardando los siguientes aspectos de estas:

Autenticidad: Permite asegurar que la información no fue modificada durante su recolección y es totalmente original.

[58] COLOMBIA. SENADO DE LA REPÚBLICA. Ley 1581. (17, octubre, 2012) protección de datos personales. Por la cual se imparte instrucciones relacionadas con la explotación de datos. Bogotá. p. 68.

Cadena de custodia: Permite asegurar que la evidencia recolectada es confiable para respaldar un proceso judicial acusatorio de un trabajador o contratista que haya cometido un delito informático.

Validación: Acción realizada con el fin de certificar que la información es la misma que se recolectó inicialmente.[59]

Aspectos Generales:

Se definirá un responsable de la protección de datos, quien se encargará de determinar el periodo de retención para cada activo de información dependiendo de su clasificación.

Por otra parte, se tendrá en cuenta como parte del periodo de retención de información todas aquellas solicitudes realizadas por externos basadas en órdenes judiciales o por necesidad propia de la organización, para estos casos se deberá contar con una justificación suficientemente relevante y bien definida.

Se tendrá una retención de 5 años para la información que no se encuentre registrada en la tabla de retención del CSIRT - UNAD.

Se deberán conservar los datos durante todo el tiempo de retención velando por su conservación teniendo en cuenta todos los formatos en los que se encuentra la información como son físico y digital, para ello se deberán disponer espacios óptimos para la conservación de los contenedores de la información.

La persona encargada de la protección de datos será la responsable de garantizar que todos los colaboradores del CSIRT - UNAD en sus diferentes dependencias, cumplan con

[59] DELVASTO RAMÍREZ, Ramiro Andrés. Modelo de gestión de incidentes de seguridad de la información para pymes. [En línea]. Universidad nacional abierta y a distancia (UNAD). 2016 [Consultado: 14 de julio de 2021]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/6170/11324611.pdf?sequence=1&isAllowed=y

la política de retención de manera correcta, asesorándolos en las actividades que deban ser desarrolladas por ellos.

El no cumplir con las definiciones determinadas en esta política conllevará una acción disciplinar a todo aquel que sea participe del hecho, dicha investigación y sanción será avalada por el responsable de protección de datos en acuerdo con el área de gestión humana.

Responsabilidades:

La persona encargada de la protección de datos será la responsable de garantizar que todos los colaboradores del CSIRT - UNAD en sus diferentes dependencias, cumplan con la política de retención de manera correcta, asesorándolos en las actividades que deban ser desarrolladas por ellos.

Todos los colaboradores deben cumplir con lo establecido en la política de retención de información.

5.7.4. Política de destrucción de información

Objetivo: Establecer 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.

Alcance: El presente documento contiene los lineamientos generales sobre los pasos y acciones a seguir para eliminar información clasificada como confidencial y/o depurar los medios que la contienen; cuando han terminado su ciclo de vida.

Aplica para medios magnéticos y electrónicos e información digital de los funcionarios, contratistas o terceros que el CSIRT - UNAD tenga en su poder, garantizando que la información sea eliminada de forma segura y que no pueda ser recuperable posteriormente.

Definiciones:

Activo de Información: Se refiere a cualquier elemento tecnológico, físico o intangible que almacena, procesa o genera información y es de valor para la compañía; algunos ejemplos de ellos son, los programas, las personas, los archivos digitales, los documentos físicos impresos, la infraestructura tecnológica, entre otros.

Estos activos pueden existir de diferentes maneras como videos, almacenamiento electrónico, de forma impresa, en el conocimiento de las personas, en archivos de audio…

Borrado Seguro: Hace referencia a cómo asegurar que la información contenida en un medio de almacenamiento, no se pueda recuperar por medio de alguna técnica u herramienta especializada de recuperación de datos.

Borrado Común: Se refiere al método común y normalmente utilizado en los sistemas operativos para llevar a cabo el borrado de la información, este consiste en hacer una nueva definición de los punteros asociados a los sectores que guardan datos como sectores libres, sin embargo, dicho marcado, no garantiza que la información contenida en los sectores se borre de manera inmediata, lo que permite que la misma pueda ser recuperada por medio del uso de herramientas especializadas en el escaneo de los medios de almacenamiento.

Aspectos Generales:

Eliminación o Depuración de Información

Una vez se ha determinado que la información o el medio de almacenamiento ha cumplido su ciclo de vida, se debe proceder a eliminarlo o depurarlo de forma segura.

Criterios de Decisión

Los funcionarios o dueños de la información deben considerar y/o evaluar criterios predefinidos para tomar la decisión de depurar o eliminar la información contenida en medios de almacenamiento o en recursos tecnológicos de CSIRT - UNAD.

Algunos de los criterios a ser considerados (pero sin limitarse a):

- Vencimiento de tiempo establecido en las Tablas de Retención (conservación) de información del CSIRT – UNAD.
- Obsolescencia del medio de almacenamiento, considerando el costo de mantenimiento (proveedor de servicio), la probabilidad de continuar siendo utilizado.
- Reutilización de los medios al interior de CSIRT - UNAD (PCs, servidores u otros).
- Cambio de proveedor de servicios informáticos y/o de centro de cómputo o procesamiento (hosting, servicios de TIC).
- Cambio de proveedor de servicio de custodia externa, alquiler y/o leasing de equipos.

Aplicabilidad

Todos los recursos tecnológicos, medios y/o dispositivos almacenamiento incluyendo dispositivos extraíbles o removibles de almacenamiento como son las memorias USB/Flash, tarjetas SD, tarjetas microSD, discos duros portátiles, CD/DVDs regrabables, dispositivos electrónicos como tabletas, celulares, entre otros, que contengan información

y/o datos (sin importar el formato), que vayan a ser dados de baja, destruidos o reutilizados.

En caso de existir información del CSIRT - UNAD almacenada en medios o recursos tecnológicos de terceros o externos al servicio del CSIRT - UNAD, se debe requerir a los terceros ejecutar procedimientos o actividades de borrado seguro de información, cumpliendo con los requerimientos y/o definiciones de CSIRT - UNAD, en cuanto a herramientas y algoritmos o métodos de borrado o eliminación.

Las técnicas de borrado seguro y depuración; así como destrucción aplican para los medios que almacenan información clasificada como confidencial- datos personales sensibles (Ley 1581/2012).

Para otras clasificaciones de información como uso interno y/o público se puede utilizar las técnicas de borrado normal.

Cumplimiento Medio Ambiental

Los métodos seleccionados para la realización de depuración o eliminación de información o medios deben cumplir con las normas y aspectos regulatorios en materia medio ambiental, que apliquen al CSIRT - UNAD.

Herramientas o Tecnologías Autorizadas para el Borrado

Las herramientas y algoritmos o métodos de borrado lógico a ser utilizados deben corresponder con las definidas, autorizadas y comunicadas por el CSIRT - UNAD; considerando tipo de medio o dispositivo, alguna de ellas puede ser:

Norma de los Estados Unidos DoD 5220-22M

Consiste en primer lugar, en escribir sobre el soporte con un valor fijo establecido, luego, con un segundo valor complementario y por último con valores aleatorios, el método consta de tres sobre escrituras y tres validaciones.

Norma de Canadá RCMP TSSIT OPS-II

A diferencia de la anterior norma en esta se sobre escribe el disco siete veces y se hacen siete verificaciones lo que asegura que la información original del disco no pueda ser recuperable.

El estándar de la OTAN

Se sobre escribe el disco en siete veces, las seis primeras, con valores fijos diferentes entre cada sobreescritura y la última con valores aleatorios.

Datos Pseudoaleatorios:

Se usa un algoritmo llamado ISAAC, con el que se generan números de forma pseudoaleatoria y también el flujo que nombra el generados, lo más relevante de este estándar es que el usuario puede seleccionar cuantas veces quiere aplicar la sobre escritura al disco hasta un tope de 65535 veces.

Método Gutmann

Es uno de los métodos más seguros ya que a diferencia de los anteriores, se realizan las primeras cuatro pasadas de sobre escritura aleatoria sobre cada sector del disco utilizando el algoritmo ISAAC para la generación de números aleatorios, luego se realizan 27 sobre escrituras adicionales, y al final se realizan otras cuatro sobreescrituras

aleatorias en cada sector, para un total de 35 patrones de sobreescritura.[60]

Para la destrucción de dispositivos y medios físicos, se deberá garantizar que los métodos utilizados no permitan la obtención o reconstrucción parcial o total de la información en ellos contenida.

Archivos y Carpetas en Servidores Windows

Los archivos y carpetas se borren de manera segura pueden hacerlo por medio del comando *"sdelete"* o de cualquier otra herramienta de borrado segura especializada que permita generar evidencia del proceso. Para el borrado de espacio no usado puede utilizarse el comando *"cipher /w"* o cualquier otra herramienta especializada que permita generar evidencia y cumpla con el procedimiento de borrado mínimo solicitado.

En caso de realizarse el borrado seguro por medio de comandos, se debe tomar evidencia (por medio de log de sistema o imagen del resultado en pantalla) de este borrado donde quede clara la fecha y hora del borrado, el archivo o carpeta eliminada, que el proceso fue completado sin errores y el formato de borrado (puede ser el utilizado por defecto).

Archivos y Carpetas en Servidores Linux/Aix/Solarix

Los archivos y carpetas que se borran de manera segura pueden realizarse con los comandos *"srm"* o *"shred"* o utilizando una herramienta de borrado seguro especializada.

El borrador de espacio en blanco se puede realizar por medio del *comando "sfill"* o por medio de herramientas de wipe especializadas.

[60] GARCIA PABON, Jhon Jairo. Borrado seguro de información en discos duros. [en línea]. Bogotá (Colombia). Universidad Piloto de Colombia [Consultado: 14 de julio de 2021]. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2982/00001165.pdf?sequence=1

Evidencia: En caso de realizarse el borrado seguro por medio de comandos, se debe tomar evidencia (por medio de log de sistema o imagen del resultado en pantalla) de este borrado donde quede clara la fecha y hora del borrado, el archivo o carpeta eliminada, que el proceso fue completado sin errores y el formato de borrado (puede ser el utilizado por defecto).

Archivos y Carpetas en Bases de Datos

Las columnas o campos que contengan datos que superen los tiempos de retención o ya no sean requeridos, deben ser eliminados de manera segura con alguna de las siguientes opciones:

Eliminación segura de la tabla, la columna o el campo por medio de comandos propios de borrado seguro del motor de base de datos (que garanticen como mínimo un estándar de tres escrituras y su posterior borrado).

Realizar la escritura en los campos que contengan número de tarjeta primero con 16 ceros, luego con 16 unos y por último con 16 dígitos aleatorios.

Registros

El CSIRT - UNAD y los responsables de ejecutar las actividades de eliminación y depuración deben registrar cada ejecución o eliminación de medios realizada en el que se debe contemplar: los medios depurados o eliminados, usuario que realizó el proceso, fecha y método (manual, automático), así como la herramienta utilizada.

Cada responsable de la información debe estar presente al momento de realizar la documentación en un acta de destrucción de un activo de información.

Eliminación de Datos en Medios Lógicos

Al momento de seleccionar un método de depuración o borrado de información se debe considerar alguna de las siguientes opciones, garantizando que los medios de almacenamiento y/o recurso tecnológico se mantenga operativo y que pueda ser reutilizable:

- Limpiar
- Purgar
- Destruir

Destrucción Física de Información o Medios.

En el caso de que la eliminación lógica de la información no se realice correctamente por fallo del dispositivo, esta situación debe documentarse y analizar la utilización de métodos de destrucción física del dispositivo, asegurando que se realice cumpliendo con las normas y aspectos medioambientales.

Responsabilidades:

Responsable de la Información

El responsable de la información deberá administrarla, clasificarla y mantener su nivel de privacidad y seguridad, de acuerdo con su clasificación, valor y criticidad.

Adicionalmente, deberá establecer los usuarios que podrán tener acceso a la información y los privilegios que les serán asignados para su tratamiento, con base en criterios de segregación de funciones establecidas.

El CSIRT - UNAD es el responsable por la información de propiedad de terceros, que han depositado su información con una necesidad de negocio.

Nota: Se considerará como responsable de la información el área o funcionario de CSIRT - UNAD, a quien se le asigne algún activo de información.

La persona definida como el responsable de tratar los datos deberá apoyar y acompañar a los administradores de recursos en la ejecución de procesos de borrado seguro de información.

Realizar revisiones periódicas de los procesos de eliminación de información, con el fin de verificar que se cumplan los lineamientos definidos en este documento.

Garantizar la consecución y el suministro de los recursos requeridos para ejecutar los procesos de borrado seguro de datos o información.

5.7.5. Política de divulgación de información

Objetivo: 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.

Alcance: Es de obligatorio cumplimiento para todos los colaboradores del CSIRT - UNAD.

Definiciones:

Divulgación de información preautorizada: obtener autorización previa de parte de los clientes para compartir, por ejemplo, la información de contacto y nombres de máquinas afectadas, a otros equipos que colaboren en la para la solución oportuna de los incidentes, especialmente cuando son internacionales.[61]

[61] AUSCERT. [Sitio web]. Australia: AUSCERT, Forming an Incident Response Team. 2017. [Consultado: 14 de julio de 2021]. Disponible en: https://www.auscert.org.au/publications/forming-incident-response-team

Aspectos Generales:

Esta política se aplicará cumpliendo inicialmente con lo establecido en la POLÍTICA DE TRATAMIENTO DE DATOS del CSIRT - UNAD.

Adicionalmente, cada vez que se requiera divulgar o compartir información de los clientes del CSIRT - UNAD, bien sea por motivo de investigación judicial, colaboración profesional y cualquier situación que así lo requiera, para brindar una oportuna atención a la investigación de incidentes cibernéticos, la información debe ser compartida bajo la necesidad de conocer del receptor, únicamente se compartirá la información estrictamente necesaria para cumplir con el objetivo planteado el cual deberá ser comunicado de manera clara y justificada al custodio de los datos del CSIRT.

Algunos ejemplos claros de a quienes se les puede compartir información son:

- A otros equipos cuando la aparece una nueva vulnerabilidad no identificada anteriormente o cuando están trabajando en conjunto para solucionar un incidente.
- A sitios que son el objetivo o fuente de un ataque.
- A personas que estén realizando investigaciones judiciales
- A entidades Gubernamentales para su notificación cuando es necesario, entre otros. [62]

Adicionalmente, se deberá cumplir con lo siguiente:

Veracidad: la información suministrada deberá reflejar la realidad de la situación presentada.

[62] WEST-BROWN, Moira., et al. Service Categories. Handbook for Computer Security Incident Response Teams (CSIRTs). 2003. p. 132 -135.

Legalidad: la información suministrada deberá ser obtenida de manera legal, por medio de los permisos necesarios para ingresar en sistemas privados de ser necesario.

Oportuna: la información suministrada deberá ser entregada en el tiempo máximo requerido de una manera ágil y fluida para que sea útil y aporte valor al proceso judicial, investigación o situación específica presentada, teniendo siempre cuidado de cumplir con las normas legales en cada caso, si la información es confidencial, se deberá contar con la autorización previa de la dirección del CSIRT.

Suficiente: se deberá compartir información completa o en casos específicos toda aquella información que sea pertinente.

En caso de tener que dar declaraciones ante la prensa, la única persona autorizada para dar comunicados oficiales será el Director del CSIRT quien actuará como el vocero de la Compañía.

La información deberá ser compartida siempre por medio de los canales de comunicación seguros, acordados con el receptor, buscando siempre que la información sea protegida de ser visualizada por personas que no tengan autorización para conocerla.

Responsabilidades:

Equipo de trabajo: solicitar aprobación para compartir información confidencial en las situaciones que requieran, así como la acción misma de compartir la información.

Director del CSIRT: realizar los comunicados oficiales ante la prensa.

Coordinador CSIRT-UNAD: autorizar la divulgación de información altamente confidencial.

5.7.6. Política de acceso a la información

Objetivo: Establecer cuáles serán aquellos canales 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 la misma.[63]

Alcance: Esta política será de obligatorio cumplimiento por todo el personal del CSIRT - UNAD y está orientada a la información de los clientes del CSIRT.

Definiciones:

Factor de Autenticación: Procedimiento utilizado para validar la identidad de un usuario frente a un sistema. Los factores de autenticación pueden validar algo que se conoce (una contraseña, un PIN, entre otros), algo que se posee (Token, certificado, tarjeta inteligente o tarjeta de coordenadas entre otros) o algo que se es (lector biométrico de huella, patrones oculares, voz o verificación de patrones de escritura entre otros).

Múltiple Factor de Autenticación: Un sistema con múltiple factor de autenticación es aquel que realiza la validación de identidad mediante la utilización de más de un factor de autenticación diferente. No se considera múltiple factor de autenticación repetir la validación con el mismo método así sean diferentes valores, es decir, si digita varias contraseñas, si lee varios patrones digitales o si tiene varios dispositivos de Token.

Incidente de Compromiso de la Información: están relacionados con la afectación de la confidencialidad de la información por medio del acceso no autorizado y la publicación de esta o la afectación de la integridad de está modificándola o borrándola.

[63] ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. Buenas prácticas para establecer un CSIRT nacional. [Sitio web] Washington, D.C. (Estados Unidos) 2016 [Consultado:14 de julio de 2021]. Disponible en: https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2016/09/2016-Buenas-Practicas-CSIRT.pdf

Aspectos Generales:

Todo acceso otorgado a un trabajador y/o usuario externo, debe basarse en la necesidad de conocer, es decir, se iniciará con un modelo de restricción total y a partir de allí se brindarán los accesos estrictamente necesarios para ejecutar las labores diarias.

Usuarios Genéricos

Cada uno de los usuarios y administradores deberá contar con un identificador personal asignado y se deberá evitar que existan identificadores genéricos o compartidos que puedan dificultar la individualización de las acciones realizadas en cada componente.

Contraseñas Genéricas

Cada uno de los usuarios y administradores deberá contar con una contraseña asignada y deberá evitar reutilizarla en otros componentes de sistema. Así mismo, está prohibido tener contraseñas de grupo o compartidas que puedan dificultar la individualización de las acciones realizadas en cada componente.

Cada usuario al que se le otorgue permisos a la información almacenada en los sistemas debe establecer contraseñas seguras, que por lo menos cuenten con los siguientes parámetros, uso de caracteres especiales, letras, números, mayúsculas, signos y longitud de mínimo 8 caracteres.

Por otra parte, se prohíbe rotunamente el préstamo de los usuarios entre diferentes colaboradores o usuarios externos, todo colaborador que sea sorprendido realizando este tipo de actividad, tendrá un llamado de atención con copia en su hoja de vida, al cabo de

tres llamados de atención se entenderá como una causa justa de despido.[64]

Se establecerá un comité de acceso a la información el cual se encargará de evaluar y tomar la decisión de otorgar la autorización de los accesos a los usuarios que soliciten acceso a los sistemas de información del CSIRT.

En aquellos medios de la compañía que sean públicos como la página web, redes sociales, y canales telefónicos, únicamente se deberá divulgar información que sea categorizada como publica por motivo del acceso que tienen todas las personas sin ningún tipo de restricción, algunos ejemplos son, historia de la compañía, servicios brindados, números de contacto, noticias de la compañía, entre otros que considere pertinente el comité de acceso a la información.

Por ningún motivo se deberá publicar información que contenga datos privados.

Responsabilidades:

Responsabilidad del comité de acceso a la información:

Se encargará de evaluar y tomar la decisión de otorgar la autorización de los accesos a los usuarios que soliciten acceso a los sistemas de información del CSIRT.

Responsabilidad del administrador de los sistemas:

- Asegurar que las configuraciones de los componentes de sistema estén de acuerdo a estos estándares.

[64] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN - ICONTEC. Tecnología de la información. Técnicas de seguridad. Código de Práctica para controles de seguridad de la información. Bogotá D.C. GTC-ISO/IEC 27002. 2015. p. 20 - 22

- Evaluar y probar todos los cambios solicitados antes de su puesta en producción y validar que no afectan las condiciones de seguridad descritas en estas políticas.
- Habilitar el registro apropiado en todos los componentes de sistema de acuerdo con las directrices del comité de acceso a la información.
- Reportar incidentes de Seguridad de la Información al comité de acceso a la información.

Responsabilidad de los usuarios:

Establecer contraseñas seguras que sean seguras y cumplan con lo establecido en los requerimientos mínimos de seguridad establecidos en la política.

5.7.7. Política de uso apropiado de los sistemas del CSIRT

Objetivo: Establecer 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 los mismos únicamente para las labores de la compañía.

Alcance: Esta política estará enfocada a los sistemas de información que soportan los procesos del CSIRT y es de obligatorio cumplimiento para los administradores de los sistemas y colaboradores que utilicen los sistemas.

Definiciones:

Log de auditoría: registro de acceso restringido de las actividades realizadas en un sistema.

Segregación de funciones: actividad asociada a la separación de funciones críticas dentro de un proceso con el fin de evitar circunstancias privilegiadas para cometer fraudes.

Gestión de cambios: proceso por medio del cual se realiza el control de la aplicación de nuevas configuraciones en el ambiente productivo de un sistema y de sus nuevas versiones, con el fin de no afectar los procesos que soporta.

Aspectos Generales:

Está prohibido que los usuarios que tengan acceso a los sistemas del CSIRT los utilicen para actividades diferentes a las labores diarias que demanda su trabajo para la compañía.

Al momento de adquirir o desarrollar un sistema para el CSIRT este deberá cumplir obligatoriamente con las siguientes características, o de lo contrario no se aprobará su implementación:

- Deberá contar con un módulo para administración de usuarios, roles y privilegios.
- Deberá permitir la aplicación de contraseñas seguras y configurar políticas de parámetros mínimos de dichas contraseñas, así como controles que fuercen a los usuarios a cambiarlas cada 3 meses como máximo.
- Deberá contar con logs de auditoría que permanezcan activos y registren la actividad que cada usuario realiza en el sistema.
- Deberá contar con cifrado para las bases de datos del sistema.
- Deberá cumplir con los requerimientos legales del lugar donde se implemente.

Por otra parte, no se incluirá información en los sistemas, que no sea previamente identificada y que no cuente con un nivel de confidencialidad y se deberán realizar validaciones previas al sistema como son:

- En caso de ser desarrollado se deberá utilizar técnicas de desarrollo seguro.

- Revisar que los mensajes de error del sistema no muestren información técnica a los usuarios.
- Se deberá realizar una evaluación de vulnerabilidades y subsanarlas de ser el caso.
- Se deberá asignar una persona responsable a nivel técnico y otra a nivel funcional.
- Se deberá utilizar información ficticia para realizar las pruebas del sistema en un ambiente de pruebas.
- Se deberá contar con un repositorio en el que se almacenen las diferentes versiones del sistema el cual deberá contener controles de seguridad que impidan la modificación de las versiones.
- Se deberá contar con un licenciamiento del sistema.

Para los sistemas que han sido implementados por el CSIRT - UNAD que requieran cambios de configuración, versión, parches de seguridad, funcionalidad, se deberá surtir un proceso de gestión del cambio en el que se cuente como mínimo con lo siguiente:

- Pruebas del cambio en ambiente de pruebas.
- Ventana de tiempo en que se aplicará el cambio, la cual debe ser planeada en un momento en el que se afecte de la menor manera la operación.
- Aprobación por parte del comité de cambios.
- Plan de vuelta a atrás en caso de que falle el cambio aplicado en ambiente productivo.
- De debe contar con un sistema en el que se registrarán los cambios.

Adicionalmente, de manera mensual se deberá realizar auditoría a las actividades realizadas por una muestra de usuarios seleccionados de manera aleatoria, con el fin de validar el uso aceptable de los sistemas.

Responsabilidades:

Administrador del sistema: velar por el cumplimiento de la política en todos los aspectos técnicos mencionados.

Colaboradores del CSIRT: utilizar los sistemas de manera adecuada únicamente para las labores que demande su trabajo en el día a día.

5.7.8. Documento de Definición de Incidentes de Seguridad y Política de Eventos

Objetivo: Entender la definición de incidente de seguridad y establecer una clasificación de a cuáles se puede ver expuesto el CSIRT.

Alcance: Este documento abarcará todos aquellos incidentes de seguridad clasificados por su nivel de severidad.

Definiciones:

Evento de Seguridad de la Información: Un evento es cualquier suceso observable en un sistema, servicio o red, que indica la posibilidad de violación de la seguridad de la información del CSIRT - UNAD.

Incidente: *"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"*.[65]

Incidentes de Código Dañino: hace referencia a software que tiene como objetivo, ingresar al sistema o dañar un equipo, servidor o dispositivo de red sin que el responsable de este lo note, por ejemplo: virus, gusanos, troyanos, spyware, rootkit, ransomware,

[65] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN - ICONTEC. Ejemplo de enfoques para la categorización y clasificación de eventos e incidentes de seguridad de la información. Bogotá D.C. GTC-ISO/IEC 27035. 2015. p. 3.

herramientas de acceso remoto.

Incidentes de Política de Seguridad: violaciones a las directrices establecidas en las políticas de seguridad de la empresa por parte de los usuarios ya sea por abuso de privilegios, accesos a servicios no autorizados, sistemas desactualizados, entre otros.

Incidentes de Disponibilidad: son ataques dirigidos a dejar fuera de servicio los sistemas, dañar la imagen de la compañía atacada y/o dañar los procesos y por ende la producción por medio de denegación del servicio normal o distribuida, sabotaje, errores humanos y fallas en el software o hardware.

Incidente de Obtención de Información: son ataques pasivos que buscan obtener información relevante como el escaneo de la red para la identificación de activos y vulnerabilidades, el sniffing, la ingeniería social y el phishing.

Incidente de Fraude: fraudes realizados por medio de la suplantación de identidad utilizando Spoofing, uso de recursos y credenciales no autorizados y/o violaciones de derechos de propiedad industrial o intelectual.

Incidentes de Intrusiones: son ataques orientados a la explotación de vulnerabilidades en el diseño de la configuración o funcionamiento de los sistemas con el objetivo de ingresar de forma no autorizada a los mismos, los ejemplos de este tipo de ataque son: inyección SQL, Pharming, compromiso de cuenta de usuario, defacement, Cross-Site Scripting (XSS), ataque de fuerza bruta, inyección de ficheros remota, explotación de vulnerabilidades de software y hardware, y acceso no autorizado a la red.

Incidente de Compromiso de la Información: están relacionados con la afectación de la confidencialidad de la información por medio del acceso no autorizado y la publicación de esta o la afectación de la integridad de está modificándola o borrándola.

Incidente de Contenido Abusivo: están orientados en dañar la imagen de las compañías utilizando sus sistemas y medios electrónicos para usos ilegales como la ciberdelincuencia, acoso, extorsión y publicidad con mensajes ofensivos, violencia, pederastia, racismo, delitos y Spam.[66]

Aspectos Generales:

La categorización de los incidentes de seguridad se categorizará de acuerdo con su nivel de severidad, como se muestra en la tabla 10:

Tabla 10. Categorías para la clasificación de incidentes de seguridad de la información.

Severidad	Severidad	Ejemplos de evento de esta categoría
Bajo SEV-4 (Informacional)	No genera interrupción en los procesos del CSIRT, el incidente o evento, es detectado y se toman medidas en base a la estadística. Sensibilidad del Activo: No Crítico. Sensibilidad de Datos: Pública. Daño: Sin daño. Asistencia Experta: Ninguna, sólo acciones generales después de estadísticos. Interrupción de Servicio: No	Código malicioso detectado o SPAM y su acción bloqueada • Bloqueos por ingreso no adecuado de contraseñas. • Correos tipo Phishing (caso particular). • Intentos de sobrepasar restricciones de acceso a sitios bloqueados. • Pérdida o robo de equipamiento con información uso interno o pública.

[66] SANCHEZ GALVÁN, Alejandro. Ciberseguridad en la industria 4.0. [En línea]. Tesis de grado. Universidad Politécnica de Valencia. 2019. [Consultado: 14 de julio de 2021]. Disponible en: https://riunet.upv.es/bitstream/handle/10251/127274/S%c3%a1nchez%20-%20Ciberseguridad%20en%20la%20industria%204.0.pdf?sequence=1&isAllowed=y
https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullReport

Tabla 10. (Continuación).

Severidad	Severidad	Ejemplos de evento de esta categoría
Medio SEV-3 (Advertencia)	No genera interrupción en los procesos del CSIRT, el incidente o evento, es detectado y se puede controlar con recursos propios de la organización. Sensibilidad del Activo: No Crítico. Sensibilidad de Datos: Sólo Uso Interno. Daño: Daño Menor. Asistencia Experta: Interna. Interrupción de Servicio: Breve.	Pérdida o compromiso de una password personal o existencia de cuentas compartidas. • Correos tipo Phishing (caso masivo). y ransomware sin comprometer datos. • Uso no autorizado de un sistema. • Incumplimiento de baja severidad a Reglamento o Política de Seguridad de la Información. • Código malicioso detectado y el bloqueo de su actividad no ha sido confirmado. • Descargar, usar o compartir información de uso privado y confidencial. • Actividad sospechosa en alguna estación de trabajo no crítica. • Suplantación de correo. • Interrupción o falla, controlada, de un sistema o recurso tecnológico no crítico de la empresa.

Tabla 10. (Continuación).

Severidad	Severidad	Ejemplos de evento de esta categoría
Alto SEV-2 (Severo)	Genera interrupción durante un corto periodo en procesos del CSIRT, el incidente o evento compromete un activo importante. Sensibilidad del Activo: Crítico. Sensibilidad de Datos: Confidencial. Daño: Daño Moderado. Asistencia Experta: Interna o Externa. Interrupción de Servicio: Breve (< 1 hora).	Cambios en el hardware, firmware, software o configuraciones sin autorización. • Abuso de recursos impacta sistemas o servicios críticos. • Mal uso de recursos, instalaciones o servicios de Empresa. • Actividad de Código malicioso detectada, en curso o bloqueada, con potencial exfiltración de información de uso privado y confidencial. • Escalamiento de accesos, intento acceso no autorizado, presuntas intrusiones exitosas a un sistema, accidental o voluntario. • Movimientos sospechosos en la red, tráfico de datos • Presunta brecha de seguridad en un computador o red. Incumplimiento de alta severidad a Reglamento o Política de Seguridad de la Información.

Tabla 10. (Continuación).

Severidad	Severidad	Ejemplos de evento de esta categoría
		• Archivos maliciosos encontrados en un sistema crítico. • Interrupción o falla, controlada, de un sistema o recurso tecnológico crítico de la empresa. • Interrupción o falla, sin control, de un sistema o recurso tecnológico no crítico de la empresa. • Pérdida o robo de equipamiento con información crítica. • Acceso físico no autorizado a instalaciones de procesamiento de información crítica.
Crítico SEV-1 (Crítico)	Genera una interrupción que impacta de manera crítica la operación del CSIRT, el incidente se puede propagar rápidamente o generar daños de uno o, más activos críticos de la organización. Sensibilidad del Activo: Crítico. Sensibilidad de Datos: Confidencial. Daño: Daño Mayor.	Interrupción o falla, sin control, de un sistema o recurso tecnológico crítico de la empresa (corte de enlace, paso a productivo defectuoso, problemas hardware, error de usuario, otros). • Cambio parcial o total del sitio web, y/o aplicaciones. • Divulgación, pérdida o corrupción de datos o información críticos.

Tabla 10. (Continuación).

Severidad	Severidad	Ejemplos de evento de esta categoría
		• Defacements (alteración maliciosa) o compromisos alas páginas web de la Empresa. • Ataques DoS exitosos a través sistemas de la Empresa (al exterior) o contra sistemas de Empresa. • Código malicioso o hackeo para el cual los sistemas AVy de prevención de código malicioso no tiene respuesta o la instalación de los parches se encuentran demorada o postergada. • Explotación exitosa de un ransomware. • Cualquier violación confirmada de una ley local o internacional, o regulación aplicable a las operaciones de la Empresa. • Pérdida de la información por desastre natural, fuego, agua, falla suministro eléctrico u otros industriales.

Fuente. Elaboración propia.

Responsabilidades:

Informante: Deberá identificar y comunicar los incidentes al CSIRT por medio del canal dispuesto para ello.

Resolutor: es quien recibe el informe del incidente, lo clasifica y brinda apoyo a las medidas de resolución mientras dure una contingencia crítica, también determina las causas de los incidentes, además de generar y dar seguimiento a los planes de acción establecidos.

5.7.9. Política de gestión de incidentes

Objetivo: Normar la implementación del proceso de gestión de incidentes de seguridad de la información, para disponer de una capacidad de reacción y respuesta apropiada a estos, por parte del CSIRT - UNAD.

Alcance: Este procedimiento está dirigido a todo miembro de la organización o externo que este asociado al CSIRT, donde todos los colaboradores tienen la responsabilidad de participar en la gestión de incidentes de seguridad de la información en cualquiera de sus etapas (identificación, recepción, resolución, análisis e investigación).

Definiciones:

Gestión de incidentes de seguridad de la información: es el proceso en el cual se detecta, reportan, evalúan, responden, tratan y se aprende de los incidentes de seguridad de la información. [67]

[67] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN - ICONTEC. Ejemplo de enfoques para la categorización y clasificación de eventos e incidentes de seguridad de la información. Bogotá D.C. GTC-ISO/IEC 27035. 2015. p. 3.

IPS (Sistema de prevención de intrusiones): Es un componente de software o hardware que ejerce control en los accesos a la red para protegerla, y a los dispositivos que estén en ella, de ataques y abusos, analizando de manera detallada el tráfico de la red, y comparando constantemente los patrones de comportamiento con patrones de ataques que ya son ampliamente conocidos. Se diferencia del IDS porque al detectar un posible ataque el IPS intenta contenerlo.

Registro de eventos: Archivo de datos, conocido también como *"log de eventos"* o *"log de auditoría"* en el que un componente de hardware o software consigna las actividades realizadas automáticamente o a solicitud de un usuario u otro componente de manera inalterable.

Servicio Crítico: es un activo de información que es de vital importancia para el negocio, ya que mantiene y asegura el funcionamiento adecuado de los servicios críticos de la operación o procesos clave.

Aspectos Generales:

El procedimiento de gestión de incidentes de seguridad de la información del CSIRT de CSIRT - UNAD tomará como referencia las definiciones del *"National Institute of Standards and Technology*" en su publicación 800-61: Computer Security Incident Handling Guide. Las fases de la gestión de incidentes se definen a continuación:

Fase de Preparación

El CSIRT deberá definir y entrenar a un equipo de respuesta ante incidentes, y conseguir los recursos y herramientas necesarias para realizar la gestión de los incidentes de seguridad de la información.

Algunos recursos mínimos con los que debe contar el CSIRT para una adecuada gestión

de los incidentes son:

- Las normas, estándares y procedimientos de la organización que documentan diferentes temas relacionados con la operación diaria. La documentación técnica de instalación, operación y mantenimiento de la infraestructura de cómputo, redes y comunicaciones y herramientas de software.
- Los diagramas de red asociados a los servicios y la interrelación de sus componentes (puertos, direcciones y protocolos).
- Herramienta de detección y eliminación de virus y malware.
- Herramienta de detección y prevención de intrusos. IPS.
- Herramienta de correlación de eventos para todas las plataformas.
- Disponibilidad de personal de atención a incidentes 7x24.

Fase de Gestión del Incidente

Como parte de la gestión de los incidentes se debe realizar un monitoreo constante de los vectores de propagación como, por ejemplo:

Medios removibles: Incidentes que se propagan a través de periféricos o medios de almacenamiento removibles.

Desgaste, Erosión o Daño: Incidentes que se originan a través de ataques de fuerza bruta para impactar, disminuir o romper los sistemas, las redes o los servicios de la organización.

Web: Ataques originados hacia sitios web o aplicaciones que expongan servicios a través de internet.

EMAIL: Ataques originados a través de correos electrónicos o sus adjuntos.

Suplantación: Ataque que implica la sustitución de elementos conocidos con otros fraudulentos con fines maliciosos.

Uso Inadecuado: Incidentes que resultan de la violación de las políticas que brindan los lineamientos del uso adecuado de los recursos por parte de un usuario que ha sido autorizado de manera previa.

Pérdida o robo de equipos: Incidentes originados por el extravío o robo de equipos de cómputo, dispositivos o medios de almacenamiento removible.

Otros: cualquier incidente originado por otros medios diferentes a los descritos anteriormente.

Por otra parte, las fuentes autorizadas para la detección y reporte de posibles incidentes de seguridad de la información son:

Personal del csirt: Cuando una persona que trabaja directamente con el equipo de respuesta a incidentes cibernéticos de CSIRT - UNAD. o cualquiera de sus terceros relacionados realiza un reporte formal y documentado de un incidente de seguridad de la información.

Cliente del csirt: Cuando una persona que trabaja para una de las empresas clientes del equipo de respuesta a incidentes cibernéticos de CSIRT - UNAD. hace un reporte de un incidente de seguridad de la información.

Correlacionador De Eventos: Cuando la herramienta dispuesta por el CSIRT para la recolección, análisis, almacenamiento y correlación de registros de auditoría (logs) genere una alarma de posible incidente de seguridad de la información.

Registro del incidente

Al presentarse alguno de los incidentes descritos en el *"DOCUMENTO DE DEFINICIÓN DE INCIDENTES DE SEGURIDAD Y POLÍTICA DE EVENTOS CSIRT-D-001"*, se generará un registro de este en los formatos dispuestos para ello.

Fase de Análisis:

Luego de ser registrado el incidente de seguridad de la información deberá ser categorizado con base en lo establecido en el *"DOCUMENTO DE DEFINICIÓN DE INCIDENTES DE SEGURIDAD Y POLÍTICA DE EVENTOS"*.

En primera instancia el administrador del correlacionador de eventos, o quien reciba la alerta de incidente de seguridad, debe realizar un análisis minucioso del evento apoyándose en las áreas implicadas para determinar si corresponde o no a un incidente. Una vez que determine que puede corresponder a un incidente, deberá revisar los procedimientos específicos para dar una posible solución o escalarlo de acuerdo con dicho procedimiento definido para cada tipo de incidente.

Documentación de Incidentes de seguridad de la información

Una vez se definido un incidente de seguridad de la información, se debe solicitar al equipo técnico relacionado que comience el seguimiento exhaustivo de los eventos que pueden completar la información necesaria para dar solución efectiva al incidente.

Todas las actividades deben quedar completamente documentadas, desde su solicitud hasta la información resultante de su ejecución.

Es responsabilidad del comité de gestión de incidentes de seguridad, o de quien este designe para tal fin, salvaguardar la información de los incidentes, restringiendo el acceso y almacenándola de manera segura.

Notificación de Incidentes de seguridad de la información

Cuando el análisis realizado por el Comité de Gestión de Incidentes arroja que un reporte corresponde efectivamente a un incidente, el comité tiene la obligación de notificar a las áreas involucradas el hecho.

Si el incidente de seguridad involucra terceros o entidades externas al CSIRT, el comité debe establecer los canales de comunicación adecuados para el informe de incidente y la coordinación de la gestión.

Fase de Contención, Erradicación y Recuperación

Contención:

Para los incidentes conocidos se deberán establecer procedimientos definidos que ayuden al personal de CSIRT a dar respuesta de manera más rápida a los mismos, estos procedimientos deberán ser actualizados periódicamente.

Al momento de establecer las medidas de contención el comité de gestión de incidentes deberá tomar la decisión de cuál es la mejora acción, algunas de ellas pueden ser:
Apagar un equipo o servidor.

Desconectar un equipo, servidor o componente de la red. Bajar, suspender o inhabilitar un servicio o recurso.

Algunos de los criterios que deben tener en cuenta son:

- Posible daño o pérdida de información o recursos.
- La necesidad de preservar o no evidencia del incidente.

- La disponibilidad total del servicio
- El tiempo aproximado que se requiere para implementar la estrategia.
- El nivel de contención de las acciones (contención parcial o total del incidente) Duración de las medidas adoptadas (contención por horas, días o solución permanente).

Erradicación:

Una vez contenido un ataque o incidente, es necesario identificar los componentes involucrados para así eliminarlos. El Comité de Gestión de Incidentes del CSIRT, debe coordinar a las áreas o equipos técnicos y funcionales para identificar dichos componentes y proceder a su eliminación o corrección.

Algunas de las actividades pueden ser:

Eliminación de software comprometido. Eliminación de malware.
Inhabilitación, actualización o eliminación de cuentas de usuario comprometidas.

Del mismo modo, las áreas involucradas deben identificar cuáles fueron las vulnerabilidades explotadas para su debida remediación.

Recuperación:

En la recuperación, las áreas técnicas o funcionales involucradas en el incidente deberán confirmar al Comité de Gestión de Incidentes del CSIRT, que las acciones de erradicación fueron exitosas y que los componentes están funcionando correctamente. Dicha confirmación deberá estar acompañada por las pruebas técnicas y funcionales.

Las actividades de recuperación pueden ser:

- Restauración parcial o total de copias de seguridad (backups) no comprometidas. Reconstrucción de los sistemas (reinstalación completa).
- Cambio de software o archivos que fueron comprometidos con versiones libres de malware.
- Instalación de parches de seguridad.
- Endurecimiento de la seguridad (reglas de firewall, listas de control de acceso y hardening de dispositivos entre otros).
- Cambio de contraseñas.

Una vez se hayan tomado las acciones pertinentes, el incidente debe cerrarse y dejar registrado todo el procedimiento realizado, las acciones realizadas y demás hechos o datos relevantes.

Responsabilidades:

Responsabilidad del Comité de Gestión de Incidentes:

- Analizar los eventos asociados al incidente de Seguridad de la Información para determinar su veracidad (que no es un falso positivo) y priorización.
- Coordinar el escalamiento entre las áreas involucradas en el incidente para determinar las actividades de contención, erradicación y remediación a realizar, notificar a las marcas de pagos (sólo si se vieron involucradas), así como las actividades posteriores a su solución.
- Analizar periódicamente los incidentes de seguridad ocurridos para identificar oportunidades de mejora y posibles actividades que puedan reducir la recurrencia de incidentes.
- Reunirse o sesionar cada vez que se presente o se determine un incidente de seguridad de la información.

5.7.10. Política de cooperación

Objetivo: 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.

Alcance: Está política debe ser cumplida por todos los trabajadores del CSIRT, abarca los acuerdos de cooperación entre entidades para la trabajar de manera conjunta obtener mejores resultados al momento de investigar y/o actuar ante incidentes de seguridad de la información.

Definiciones:

Cooperación para la gestión de incidentes de seguridad de la información: acuerdos predefinidos entre el equipo de respuesta a incidentes de la compañía CSIRT - UNAD. Con otros CSIRT y compañías de seguridad de la información para el análisis, contención y respuesta ante los incidentes de seguridad de la información.

Aspectos Generales:

Como parte de los acuerdos mínimos predefinidos entre el equipo de respuesta a incidentes de la compañía CSIRT - UNAD. con otros CSIRT y compañías de seguridad de la información para el análisis, contención y respuesta ante los incidentes de seguridad de la información, se establecen:

Se debe contar con un acuerdo previo entre las entidades el cual debe estar firmado y en el que se determinen claramente los objetivos de la cooperación.

Se debe compartir información únicamente con el fin de colaborar con el análisis, contención y respuesta de los incidentes de seguridad de la información.
El acuerdo debe ser claro respecto a las condiciones de terminación de la cooperación.
Las entidades que cooperarán deben comprometerse a guardar todo lo establecido en la *"POLÍTICA DE PROTECCIÓN DE DATOS"*

Responsabilidades:

Es responsabilidad de todos los colaboradores del CSIRT conocer las condiciones de cooperación establecidas en esta política y actuar conforme a cada una de ellas.

5.7.11. Política del Cumplimiento de la Ética y la Confidencialidad

Objetivo: 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.

Alcance: Está política debe ser cumplida por todos los trabajadores del CSIRT, abarca los aspectos éticos y comportamentales que deben tener los Profesionales de la Seguridad de la Información del CSIRT-UNAD al interior del CSIRT y hacia las comunidades objetivo del mismo.

Definiciones:

Ética profesional: Se define como aquellos valores universales para el ser humano y que se aplican al entorno laboral.
Trabajo en equipo: Labor que se lleva a cabo por medio de varios integrantes y que responde a un objetivo en común, pero con actividades individuales que son desarrolladas por cada uno de los miembros.

Código de ética: Conjunto de normas, las cuales tienen por objetivo regular los comportamientos de las personas que hacen parte de un mismo contexto, esto basado en una aplicación de valores y rectitud moral.

Aspectos Generales:

Los Profesionales de la Seguridad de la Información del CSIRT-UNAD deberán tener compromiso con el trabajo, cumpliendo con las actividades asignadas en los tiempos establecidos y con la mejor calidad posible para agregar el valor esperado a las partes interesadas.

Los Profesionales de la Seguridad de la Información del CSIRT-UNAD deberán tener una conducta y ética profesional, adoptando los valores éticos y morales, actuando siempre en pro del beneficio colectivo y buscando el cumplimiento de las leyes gubernamentales, también deberán cumplir con lo establecido en el código de ética de la Universidad Nacional Abierta y a Distancia, UNAD y el código de ética del Consejo Profesional Nacional de Ingeniería, COPNIA.

Los Profesionales de la Seguridad de la Información del CSIRT-UNAD deberán trabajar en equipo, buscando el mejoramiento continuo y el cumplimiento de los objetivos trazados a corto plazo en el plan de trabajo diario y a largo plazo en la estrategia definida para el CSIRT UNAD, siempre en pro de lograr lo establecido en la misión y la visión del CSIRT.

Los Profesionales de la Seguridad de la Información del CSIRT-UNAD se comprometerán con el fomento de la educación, cultura y concienciación de las comunidades objetivo, brindando en todo momento información actual y verdadera que ayude a la comunidad académica a comprender y apropiar toda la terminología y buenas prácticas de la seguridad de la información como un habito de vida.

Los Profesionales de la Seguridad de la Información del CSIRT-UNAD deberán comprometerse con las reglas establecidas en el trabajo, procurando así un ambiente agradable y ameno para la realización de actividades laborales.

Los Profesionales de la Seguridad de la Información del CSIRT-UNAD deberán tener compromiso con el respeto, disciplina, concertación y conciliación como valores fundamentales y promoverán y harán que se respete el Código de Ética.

Por ningún motivo se permite a los colaboradores del CSIRT aceptar cualquier regalo, obsequio, ni dinero en efectivo, que pueda motivar a la omisión o realización inadecuada de actividades propias a la gestión de incidentes de seguridad de la información y/o actividades de los servicios brindados por el CSIRT - UNAD.

Compromisos de los profesionales de seguridad de la información del CSIRT - UNAD frente a las comunidades objetivo del mismo:

Deberán utilizar su conocimiento y habilidades a favor de la comunidad académica, absteniéndose de hacer daño a la misma, buscando satisfacer las necesidades de esta por medio de su rol en el CSIRT – UNAD.

Deberán ser honestos y promover en todo momento la confianza en las comunidades a las que se les ofrecen los servicios del CSIRT – UNAD, por medio de actos coherentes que demuestren una conexión única entre lo que se piensa, se habla y se hace, siempre buscando cumplir con lo acordado en cada trabajo.

Deberán ser responsables e identificar si se tienen las capacidades para realizar el trabajo encomendado, en caso de identificar que no se cuenta con el conocimiento y la habilidad para realizarlo, se deberá comunicar de inmediato a su jefe con el fin de identificar si se requiere apoyo de un tercero que brinde dichos servicios específicos,

siempre buscando realizar un trabajo adecuado, de calidad y que cumpla con los objetivos establecidos.

Deberán tratar la información que le ha confiado la comunidad velando por mantener en todo momento su privacidad y confidencialidad, lo anterior por medio del cumplimiento de lo estipulado en la política de protección de datos del CSIRT – UNAD y a través de la ejecución de los controles asociados a cada activo de información.

Los colaboradores deberán abstenerse de dar declaraciones de cualquier tipo acerca de información que maneja el CSIRT, dicha actividad la deberá realizar únicamente la persona que en su momento tenga el rol de vocero del CSIRT – UNAD.

Deberán utilizar los recursos tecnológicos del CSIRT – UNAD de manera adecuada cumpliendo con lo establecido en la política de uso apropiado de los sistemas del CSIRT.

Deberán aportar al crecimiento integral del equipo de trabajo del CSIRT- UNAD y a las comunidades objetivo del mismo a través del conocimiento adquirido sin restricción y apoyando en las actividades que tanto los compañeros de trabajo, como la comunidad no puedan realizar por si mismos, siempre y cuando se cuente con lo necesario para brindar dicho apoyo y haga parte de los servicios ofrecidos por el CSIRT – UNAD.

Responsabilidades:

Es responsabilidad de todos los colaboradores del CSIRT conocer las condiciones de cooperación establecidas en esta política y actuar conforme a cada una de ellas.

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 el Centro de Respuesta a Incidentes Informáticos CSIRT-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.

RECOMENDACIONES

La ciberdelincuencia ha crecido a la par de la sociedad digital por lo que deben tomarse medidas de precaución que anticipen el actuar de los ciberdelincuentes y permitan dar una oportuna respuesta a los incidentes cibernéticos, al respecto, es recomendable establecer políticas principales que brinden los lineamientos al interior de los Centros de Respuesta a Incidentes Cibernéticos CSIRT del sector académico, que permitan a los profesionales de TI resguardar la integridad, confidencialidad y disponibilidad de la información ante cualquier posible ataque cibernético bien sea realizado desde el interior de las instituciones o desde el exterior.

Es necesario que todos los miembros que participan de los servicios reactivos y proactivos que brinda el CSIRT de la Universidad Nacional Abierta y a Distancia – UNAD, conozcan las políticas definidas para la actuación del mismo, esto se puede lograr por medio de la capacitación de los profesionales de TI una vez sean vinculados al CSIRT, de manera presencial o por medio de cursos virtuales, adicionalmente, es recomendable contar con un repositorio centralizado en el que reposen las políticas actualizadas al cual deben tener acceso estos profesionales.

Es importante contar con un proceso de mejora continua que permita mantener los lineamientos de actuación claros con el paso del tiempo para no desviarse de los objetivos estratégicos definidos por la dirección, por lo anterior, es recomendable para el CSIRT de la Universidad Nacional Abierta y a Distancia – UNAD, definir un tiempo de

revisión y actualización de las políticas principales que permiten dar desarrollo a sus actividades, teniendo como base cambios significativos en la regulación vigente, en los procesos y servicios, en la misión y visión del CSIRT.

BIBLIOGRAFÍA

AGENCIA DE PERIODISMO INVESTIGATIVO. [Sitio web]. Bogotá: Agencia de periodismo investigativo. Universidad del Bosque bajo ataque cibernético. [Consultado:14 de julio de 2021]. Disponible en: https://agenciapi.co/noticia/academia/universidad-del-bosque-bajo-ataque-cibernetico

ALCALDÍA DE BOGOTÁ. [Sitio web]. Bogotá: ALCALDÍA DE BOGOTÁ, Ubicación de la Ciudad [Consultado: 14 de julio de 2021]. Disponible en: https://bogota.gov.co/ubicacion-de-bogota-sitios-turisticos-vias-y-alrededores-de-bogota

ASOBANCARIA. [Sitio web]. Bogotá: ASOBANCARIA, Implementación y puesta en marcha CSIRT para el sector financiero 2017. [Consultado: 14 de julio de 2021]. Disponible en: https://www.asobancaria.com/wp-content/uploads/CSIRT-Financiero-Asobancaria-julio-2018.pdf

AUSCERT. [Sitio web]. Australia: AUSCERT, Forming an Incident Response Team. 2017. [Consultado: 14 de julio de 2021]. Disponible en: https://www.auscert.org.au/publications/forming-incident-response-team

BERDUGO SIERRA, Helber Alirio. Importancia de definir la infraestructura critica en Colombia. [En línea]. Tesis de especialización. Universidad Militar Nueva Granada. 2016. [Consultado: 14 de julio de 2021]. Disponible en:

https://repository.unimilitar.edu.co/bitstream/handle/10654/14342/BerdugoSierraHelber%20Alirio2016.pdf?sequence=1&isAllowed=y

BRICKER & ECKLER LLP. [Sitio web]. Bricker & Eckler LLP. Privacy & Data Protection. 2015 Cybersecurity Seminar. [Consultado:14 de julio de 2021]. Disponible en: https://www.bricker.com/industries-practices/privacy-data-protection/insights-resources/resource/2015-cybersecurity-seminar-783

CAROZO, Eduardo; MARTINEZ, Carlos. VIDAL, Leonardo. CERTuy: Hacia un CSIRT Nacional [Sitio web] 2020 [Consultado:14 de julio de 2021]. Disponible en: https://iie.fing.edu.uy/eventos/telcom2006/trabajos/mvdtelcom-013.pdf

CASANOBA Romeo y CARLOS María, Poder informático y Seguridad jurídica, Editorial Fundesco. Madrid. 1988. ISBN 10: 8486094321

CAVIEDES SANABRIA, Fernando y PRADO URREGO, Bertulfo. Modelo unificado para identificación y valoración de los riesgos de los activos de información en una organización. [En línea]. Universidad ICESI. 2012. [Consultado: 14 de julio de 2021]. Disponible en: https://pdfs.semanticscholar.org/c8a0/cc6a02ce0b801df4442a32e1bc8e67f20cc2.pdf

CHANCHA CHUNATA, Mónica. Análisis de las metodologías ENISA y APCERT para la creación del centro de respuesta a incidentes informáticos (CSIRT). Caso práctico: prototipo de un CSIRT en la universidad nacional de Chimborazo. [En línea]. Universidad nacional de Chimborazo 2019. [Consultado: 14 de julio de 2021]. Disponible en: http://dspace.unach.edu.ec/bitstream/51000/6284/1/AN%c3%81LISIS%20DE%20LAS%20METODOLOG%c3%8dAS%20ENISA%20Y%20APCERT%20PARA%20LA%20CREACI%c3%93N%20DEL%20CENTRO%20DE%20RESPUESTA.pdf

CIBERSEGURIDAD LATAM. [Sitio web]. CIBERSEGURIDAD LATAM. Kaspersky registra 45 ataques por segundo en América Latina. 2020. [Consultado: 14 de julio de 2021]. Disponible en: https://www.ciberseguridadlatam.com/2019/08/29/kaspersky-registra-45-ataques-por-segundo-en-america-latina/

COLOMBIA. CONGRESO DE COLOMBIA. Ley 1273. (5, enero, 2009). Por la cual se imparte instrucciones relacionadas con los delitos informáticos. Bogotá DC. p. 1 - 2.

COLOMBIA. DEPARTAMENTO NACIONAL DE PLANEACIÓN. Política nacional de explotación de datos (Big data) CONPES 3920. Por la cual se imparte instrucciones relacionadas con la explotación de datos. (17, abril, 2018). Bogotá DC. p. 19 - 21.

COLOMBIA. DEPARTAMENTO NACIONAL DE PLANEACIÓN. Política nacional de seguridad digital. Por la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones (11, abril, 2016). Bogotá DC. p. 30 - 46.

COLOMBIA. SENADO DE LA REPÚBLICA. Ley 1581. (17, octubre, 2012) protección de datos personales. Por la cual se imparte instrucciones relacionadas con la explotación de datos. Bogotá. p. 68.

COLOMBIA. SUPERINTENDENCIA FINANCIERA DE COLOMBIA, Circular externa 007, (5, junio, 2018). Por la cual se imparte instrucciones relacionadas con los requerimientos mínimos para la gestión del riesgo de ciberseguridad. Bogotá DC. 20 p.

CORTÉS BORRERO, Rodrigo. Estado actual de la política publica de ciberseguridad y ciberdefensa en Colombia. [En línea]. Universidad Santo Tomas. 2015. [Consultado: 14 de julio de 2021]. Disponible en:

https://repository.usta.edu.co/bitstream/handle/11634/14032/2015rodrigocortes.pdf?cv=1&sequ

DE LA TORRE MOSCOSO, Hugo y PARRA ROSERO, Mario. Estrategia y diseño de un equipo de respuesta ante incidentes de seguridad informática (CSIRT) académico para la universidad de las fuerzas armadas ESPE. [En línea]. Universidad de las Fuerzas Armadas. 2018. [Consultado: 14 de julio de 2021]. Disponible en: http://repositorio.espe.edu.ec/bitstream/21000/15071/1/T-ESPE-040447.pdf

DELVASTO RAMÍREZ, Ramiro Andrés. Modelo de gestión de incidentes de seguridad de la información para pymes. [En línea]. Universidad nacional abierta y a distancia (UNAD). 2016 [Consultado: 14 de julio de 2021]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/6170/11324611.pdf?sequence=1&isAllowed=y

EL ESPECTADOR. [Sitio web]. Bogotá: EL ESPECTADOR. Anonymous ataca el sitio web de la Universidad de los Andes. [Consultado:14 de julio de 2021]. Disponible en: https://www.elespectador.com/actualidad/anonymous-ataca-el-sitio-web-de-la-universidad-de-los-andes-article-620617/

EL TIEMPO. [Sitio web]. Bogotá: EL TIEMPO. El cibercrimen no descansa, estas son las proyecciones para el 2020. [Consultado: 14 de julio de 2021]. Disponible en: https://www.eltiempo.com/tecnosfera/dispositivos/cifras-de-ciberataques-de-2019-y-tendencias-para-el-2020-435508

ENINSA. Cómo crear un CSIRT paso a paso. Colombia. 2006. p. 21 - 25

ESET. [Sitio web]. Welivesecurity. Falso sitio suplantaba identidad de institución financiera de Colombia para robar información de clientes. 2019. [Consultado: 14 de julio

de 2021]. Disponible en: https://www.welivesecurity.com/la-es/2019/12/20/sitio-suplanta-identidad-entidad-financiera-colombia-robar-informacion-clientes/

FIRST.ORG. Foro sobre los equipos de seguridad e intervención 2 en caso de incidente 2016. p. 8 - 10.

GARCIA PABON, Jhon Jairo. Borrado seguro de información en discos duros. [en línea]. Bogotá (Colombia). Universidad Piloto de Colombia [Consultado: 14 de julio de 2021]. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2982/00001165.pdf?sequence=1

HEREDERO, Carmen, et al. Organización y transformación de los sistemas de información en la empresa. Madrid. 2019. 431 p. ISBN 978-84-17513-74-0

HIDALGO SÁNCHEZ, Narcisa. Políticas institucionalizadas por DISENSA para incrementar franquicias en el país y en la cuidad de Machala ventajas y desventajas para los franquiciados [En línea]. Tesis de grado. Universidad Técnica de Machala. 2016. [Consultado: 14 de julio de 2021]. Disponible en: http://repositorio.utmachala.edu.ec/bitstream/48000/7861/1/ECUACE-2016-AE-CD00045.pdf

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN - ICONTEC. Tecnología de la información. Técnicas de seguridad. Código de Práctica para controles de seguridad de la información. Bogotá D.C. GTC-ISO/IEC 27002. 2015. p. 20 – 22

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN - ICONTEC. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Bogotá D.C. NTC-ISO/IEC 27001. 2015. p. 6 – 7

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN - ICONTEC. Ejemplo de enfoques para la categorización y clasificación de eventos e incidentes de seguridad de la información. Bogotá D.C. GTC-ISO/IEC 27035. 2015. p. 64 - 72.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN - ICONTEC. Compendio Seguridad de la Información – Segunda edición. 2015. 96 p. ISBN 978-958-8585-53-6

KILLCRECE, Georgia. Steps for Creating National CSIRTs. [Sitio web] Pittsburgh. 2004 [Consultado: 14 de julio de 2021]. Disponible en: https://resources.sei.cmu.edu/asset_files/WhitePaper/2004_019_001_53064.pdf

MINISTERIO DE DEFENSA. Guía de creación de un CERT / CSIRT. España. 2011. p. 43 - 45.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA [Sitio web]. Bogotá: MINTIC. Total de Suscriptores de Internet a Nivel Nacional. [Consultado: 14 de julio de 2021]. Disponible en: https://colombiatic.mintic.gov.co/679/w3-propertyvalue-47275.html

MORALES GONZALEZ, Ricardo. Un modelo efectivo para la administración de incidentes de seguridad de la información. [diapositivas]. Bogotá. 12 diapositivas. [Consultado: 14 de julio de 2021]. Disponible en: http://isacamty.org.mx/archivo/133-Mejores_Practicas_la_Admin_de_Incidentes.pdf

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. Buenas prácticas para establecer un CSIRT nacional. [Sitio web] Washington, D.C. (Estados Unidos) 2016 [Consultado:14 de julio de 2021]. Disponible en: https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2016/09/2016-Buenas-Practicas-CSIRT.pdf

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. Impacto de los incidentes de seguridad digital en Colombia. Colombia. 2017. p. 48 - 91.

PROYECTOAURORAONG. [Sitio web]. PROYECTOAURORAONG. Como crear un CSIRT Fundamentos. [Consultado: 14 de julio de 2021]. Disponible en: https://www.youtube.com/watch?v=2huboveQFLs

RAMÍREZ LUNA, Helton y MEJIA MIRANDA. Jezreel. Propuesta de infraestructura técnica de seguridad para un Equipo de Respuesta ante Incidentes de Seguridad (CSIRT). [en línea]. Zacatecas (México): Universidad de Guadalajara 2015. [Consultado: 14 de julio de 2021]. Disponible en: https://www.redalyc.org/articulo.oa?id=512251501006

SANCHEZ GALVÁN, Alejandro. Ciberseguridad en la industria 4.0. [En línea]. Tesis de grado. Universidad Politécnica de Valencia. 2019. [Consultado: 14 de julio de 2021]. Disponible en: https://riunet.upv.es/bitstream/handle/10251/127274/S%c3%a1nchez%20-%20Ciberseguridad%20en%20la%20industria%204.0.pdf?sequence=1&isAllowed=y

UNIVERSIDAD NACIONAL ABIERNA Y A DISTANCIA UNAD. Plan de desarrollo 2019 – 2023. Bogotá D.C. 2018. 118 p.

UNIVERSIDAD NACIONAL ABIERTA Y ADISTANCIA UNAD. Resolución No. 0190. Bogotá D.C.: Universidad Nacional Abierta y a Distancia, 2010. 4 p.

UNIVERSIDAD NACIONAL ABIERTA Y ADISTANCIA UNAD. Resolución No. 156. Bogotá D.C.: Universidad Nacional Abierta y a Distancia, 2013. 5 p.

UNIVERSIDAD NACIONAL ABIERTA Y ADISTANCIA UNAD. Resolución No. 2110. Bogotá D.C.: Universidad Nacional Abierta y a Distancia, 2008. 15 p.

UNIVERSIDAD NACIONAL ABIERTA Y ADISTANCIA UNAD. Resolución No. 2945. Bogotá D.C.: Universidad Nacional Abierta y a Distancia, 2009. 4 p.

UNIVERSIDAD NACIONAL ABIERTA Y ADISTANCIA UNAD. Resolución No. 2943. Bogotá D.C.: Universidad Nacional Abierta y a Distancia, 2009. 3 p.

UNIVERSIDAD NACIONAL ABIERTA Y ADISTANCIA UNAD. Resolución No. 2944. Bogotá D.C.: Universidad Nacional Abierta y a Distancia, 2009. 7 p.

UNIVERSIDAD NACIONAL ABIERTA Y ADISTANCIA UNAD. Resolución No. 4793. Bogotá D.C.: Universidad Nacional Abierta y a Distancia, 2013. 18 p.

UNIVERSIDAD NACIONAL ABIERTA Y ADISTANCIA UNAD. Resolución No. 5071. Bogotá D.C.: Universidad Nacional Abierta y a Distancia, 2013. 15 p.

UNIVERSIDAD NACIONAL ABIERTA Y ADISTANCIA UNAD. Resolución No. 5303. Bogotá D.C.: Universidad Nacional Abierta y a Distancia, 2008. 9 p.

UNIVERSIDAD NACIONAL ABIERTA Y ADISTANCIA UNAD. Resolución No. 6018. Bogotá D.C.: Universidad Nacional Abierta y a Distancia, 2012. 6 p.

UNIVERSIDAD NACIONAL ABIERTA Y ADISTANCIA UNAD. Resolución No. 6858. Bogotá D.C.: Universidad Nacional Abierta y a Distancia, 2014. 5 p.

UNIVERSIDAD NACIONAL ABIERTA Y ADISTANCIA UNAD. Resolución No. 7966. Bogotá D.C.: Universidad Nacional Abierta y a Distancia, 2014. 4 p.

WEST-BROWN, Moira., et al. Service Categories. Handbook for Computer Security Incident Response Teams (CSIRTs). 2003. p. 24.

YOUTUBE. [Sitio web]. YOUTUBE. Estructura interna de un CSIRT. [Consultado: 14 de julio de 2021]. Disponible en: https://www.youtube.com/watch?v=RaBp3qsxQYY

ZAMBRANO HERMANDEZ, Luis, et al. 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" [en línea] Bogotá (Colombia) 2020 [Consultado:14 de julio de 2021]. Disponible en: https://hemeroteca.unad.edu.co/index.php/memorias/article/view/4205/4180