ESTADO ACTUAL DE LAS POLÍTICAS, PROCESOS Y PROCEDIMIENTOS RELACIONADOS CON LA SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

JANISBERTO HERRERA ZUÑIGA

Proyecto de Grado – aplicado como alternativa de trabajo de grado
para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERÍA ECBTI
ESPECIALIZACION EN SEGURIDAD INFORMATICA
FACATATIVÁ-CUNDINAMARCA
MARZO
2022

ESTADO ACTUAL DE LAS POLÍTICAS, PROCESOS Y PROCEDIMIENTOS RELACIONADOS CON LA SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

JANISBERTO HERRERA ZUÑIGA

Proyecto de Grado – aplicado como alternativa de trabajo de grado
para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Ing. Yenny Stella Núñez
Directora

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERÍA ECBTI
ESPECIALIZACION EN SEGURIDAD INFORMATICA
FACATATIVÁ-CUNDINAMARCA
MARZO
2022

NOTA DE ACEPTACIÓN

Firma del presidente de Jurado

Firma del Jurado

Firma del Jurado

Facatativá-marzo de 2022

DEDICATORIA

Con el Amor más Grande dedico este trabajo a mi familia, Mi madre: Prisca Romelia Zuñiga Gómez Q.E.P.D, a mi esposa Milena Camelo, a mis hijas: María Herrera y Alba Herrera, por sacrificar su tiempo y espacio para permitirme dedicarme a las labores que demandó este proyecto, por su apoyo incondicional en la realización y alcance de uno de los objetivos de mi vida.

Janisberto Herrera Zuñiga

AGRADECIMIENTOS

Principalmente a Dios por las oportunidades brindadas en el transcurso de nuestros aprendizajes en la permanencia dentro de la Universidad, a nuestras familias la cual es el pilar fundamental de cada esfuerzo y sacrificio, quienes estuvieron presentes en cada momento del proceso y nunca dejaron de apoyarnos emocionalmente. A cada tutor que en estos años de aprendizaje aportaron a formarnos como personas y profesionales, por cada consejo y por cada tropiezo que enseñaron a forjar nuestro carácter y tener objetivos claros día a día.

CONTENIDO

Pág.

1. INTRODUCCIÓN 17
2. PLANTEAMIENTO DEL PROBLEMA 18
2.1 ANTECEDENTES DEL PROBLEMA....18
2.2 FORMULACIÓN DEL PROBLEMA 20
3. JUSTIFICACIÓN 22
4. OBJETIVOS 23
4.1 OBJETIVO GENERAL....23
4.2 OBJETIVOS ESPECÍFICOS 23
5. MARCO REFERENCIAL....24
5.1 MARCO TEÓRICO....24
5.2 MARCO CONCEPTUAL....27
5.2.1 Seguridad de la información 27
5.2.2 Sistema de gestión de la Seguridad de la información 29
5.2.3 Familias de las Normas ISO/IEC 27000....30
5.2.4 Que Significa y que es un CSIRT.?....31
5.2.5 Tipos de CSIRT....31
5.2.6 CSIRT del sector académico. 31
5.3 MARCO HISTÓRICO 32
5.3.1 Políticas: En este segmento se observarán algunas políticas anteriormente relacionadas con la investigación sobre las políticas. 32
5.3.2 Gaviria Álvarez, Wilber Arnulfo 2017-09-27. 32
5.3.3 Ochoa Castañeda, Jaime Andres; Vela Forigua, Lina María 2018-04-01. 32
5.3.4 John Jairo Leiva Jiménez Juan Carlos Chiari Caballero-2012-11-23. 33
5.4 MARCO LEGAL....34
6. DISEÑO METODOLÓGICO....35
7. Estructura del área de tecnología de la universidad UNAD. 36
7.1 Políticas procesos y procedimientos de seguridad de la información de la UNAD. 40
8. Organización de roles, responsabilidades y funciones del centro de respuesta a incidentes informáticos Csirt-unad, políticas, procesos y procedimientos de seguridad de la información de la unad. 48
9. Formular plan maestro estratégico enfocado a la atención de eventos cibernéticos y afianzado en la cultura de ciberseguridad. 61
10. CONCLUSIONES....85
11. RECOMENDACIONES....87
12. DIVULGACIÓN....88
BIBLIOGRAFÍA 89
ANEXOS 96

LISTA DE TABLAS

Pág.

Tabla 1.Esta unidad cumplirá las siguientes funciones: 37
Tabla 2. Roles y responsabilidades área tecnologías de la información. 39
Tabla 3. Políticas Actuales En la UNAD. 40
Tabla 4. Políticas próximas en aprobación. 41
Tabla 5. Procesos PHVA UNAD. 42
Tabla 6. Definiciones, Atención de Incidentes 43
Tabla 7. Clasificación de Sensibilidad. 73
Tabla 8. Categorias de Incidentes. 74
Tabla 9. Clasificación de Criticidad del Incidente. 76
Tabla 10. Definiciones. 77
Tabla 11. Fases del Incidente. 77

LISTA DE FIGURAS

Pág.

Figura 1. Gestión de la Seguridad de la Información según ISO/IEC 17799 28
Figura 2. Principios de la seguridad informática: Confidencialidad, Integridad y Disponibilidad de la información. 29
Figura 3. Estrategia de TI de la UNAD 36
Figura 4. Organigrama Equipo Tecnología Integrada – PTI UNAD. 38
Figura 5. Explicación de la relación del CSIRT-UNAD y un SOC Prevención, respuesta y políticas de prevención. 50
Figura 6. Gráfica de jerarquización del CSIRT -UNAD 58
Figura 7 de esquema CONTROL Y CONFIANZA 59
Figura 8 de esquema CATALOGO DE SERVICIOS CSIRT-UNAD 60
Figura 9 Análisis de Riesgos 62
Figura 10 Flujograma de Procesos de atención de Incidentes. 65
Figura 11 Línea del tiempo de atención. 66
Figura 12 Análisis de Riesgos. 68
Figura 13 Sistema Sugerido de Interconexión y seguridad de red. 83
Figura 14 Diagrama de monitoreo, ciudad y estructuración CSIRT-UNAD. 84

LISTA DE CUADROS

pág.

Cuadro 1. ISO 27000 la familia de normas..... 30

LISTA DE ANEXOS

pág.

Anexo A. Nombre del Anexo 96
Anexo B. Nombre del Anexo 96

GLOSARIO

Para dar entendimiento a los términos utilizados en el presente proyecto de grado, se manifiesta que las siguientes definiciones, en su modelo de presentación se tomarán como modelo de referencia del "manual del sistema de gestión de seguridad de la información" perteneciente a la lotería nacional para la asistencia pública de México y serán empleadas en aplicación a este trabajo presentado a la Universidad Nacional Abierta y a distancia UNAD. [1]

ACTIVO DE INFORMACIÓN: de acuerdo con la norma ISO 27001, [2]un activo de información es "cualquier cosa que tenga valor para la organización y en consecuencia deba ser protegido". No obstante, este concepto es bastante amplio, y debe ser limitado por una serie de consideraciones: el impacto que para la empresa supone la pérdida de confidencialidad, integridad o disponibilidad de cada activo, el tipo de información que maneja en términos de su sensibilidad y criticidad y sus productores y consumidores. Los activos de información se traducen en dispositivos tecnológicos, archivos, bases de datos, documentación física, personas, sistemas de información, entre otros.

AUTENTICACIÓN: [3]es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

[1] DIRECCIÓN GENERAL SUBDIRECCIÓN GENERAL DE FINANZAS Y SISTEMAS. [Sitio web]. Manual del Sistema de Gestión de Seguridad de la Información. [Consulta: 12 de agosto 2021].Disponible en: M_SISTEMA_GESTION_SEGURIDAD_INFORMACION_Parte1.pdf (www.gob.mx)

[2] GAVIRIA ÁLVAREZ, Wilber Arnulfo. Propuesta de actualización de Políticas de Seguridad de la Información del Sistema de Gestión de la Información de la Empresa Caso de Estudio, en la Sede Medellín de la ISO 27001:2005 a la ISO 27001:2013. [En línea].Monografía. Universidad Nacional Abierta y a Distancia UNAD,2017. [Consulta: 12 agosto 2021]. Disponible en: https://repository.unad.edu.co/handle/10596/13274

[3] Ibid.; p.11.

CONFIDENCIALIDAD: es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados. [4]

DISPONIBILIDAD: [5]es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

DISPOSITIVOS DE ALMACENAMIENTO: [6]materiales físicos donde se almacenan datos.

DOCUMENTOS DE ACEPTACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN: [7]son documentos en los que los empleados de la Empresa caso de estudio o provistos por terceras partes aceptan acatar la Política de Seguridad de la Información y se acogen a las sanciones establecidas por el incumplimiento de dicha política.

HARDWARE: cualquier componente físico tecnológico, que trabaja o interactúa de algún modo con el computador. [8]Incluye elementos internos como el disco duro, CDROM, y también hace referencia al cableado, circuitos, gabinete, etc. E incluso a elementos externos como la impresora, el mouse, el teclado, el monitor y demás periféricos.

IP: es una dirección o etiqueta numérica que identifica, de manera lógica y jerárquica, a un interfaz (elemento de comunicación/conexión) de un dispositivo dentro de una red que utilice el protocolo IP (Internet Protocol). [9]

INCIDENTE DE SEGURIDAD: es un evento adverso, confirmado o bajo sospecha, que afecta a un sistema de información, a una red, o la violación, o inminente amenaza de violación de la Política de Seguridad de la Información. [10]

---

[4] GAVIRIA ÁLVAREZ, Wilber Arnulfo. Propuesta de actualización de Políticas de Seguridad de la Información del Sistema de Gestión de la Información de la Empresa Caso de Estudio, en la Sede Medellín de la ISO 27001:2005 a la ISO 27001:2013. [En línea].Monografía. Universidad Nacional Abierta y a Distancia UNAD,2017. [Consulta: 12 agosto 2021]. Disponible en: https://repository.unad.edu.co/handle/10596/13274

[5] Ibid.; p.11.

[6] Ibid.; p.11.

[7] Ibid.; p.11.

[8] Ibid.; p.11.

[9] Ibid.; p.12.

[10] Ibid.; p.12.

INTEGRIDAD: [11]es la confidencialidad y la exactitud en la información que es entregada y cualquier modificación no autorizada es prevenida.

OFICINA DE TECNOLOGIAS DE LA INFORMACIÓN (TI): [12]Cumple la función de cubrir los requerimientos de seguridad de la información establecidos para la operación, administración, comunicación de los recursos de tecnología de la empresa caso de estudio. Así mismo debe efectuar las tareas de desarrollo y mantenimiento de sistemas de información, siguiendo una metodología de ciclo de vida de sistemas apropiada, la cual debe contemplar medidas de seguridad.

PERFILES DE USUARIO: son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.[13]

SISTEMA DE INFORMACIÓN: es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por la Empresa caso de estudio o de origen externo ya sea adquirido por la empresa como un producto estándar de mercado o desarrollado para las necesidades de ésta.[14]

SOFTWARE: [15]es todo programa o aplicación programada para realizar tareas específicas.

SOFTWARE MALICIOSO: es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información. TIC: tecnologías de la información y las comunicaciones. [16]

---

[11] GAVIRIA ÁLVAREZ, Wilber Arnulfo. Propuesta de actualización de Políticas de Seguridad de la Información del Sistema de Gestión de la Información de la Empresa Caso de Estudio, en la Sede Medellín de la ISO 27001:2005 a la ISO 27001:2013. [En línea].Monografía. Universidad Nacional Abierta y a Distancia UNAD,2017. [Consulta: 12 agosto 2021]. Disponible en: https://repository.unad.edu.co/handle/10596/13274

[12] Ibid.; p.12.

[13] Ibid.; p.12.

[14] Ibid.; p.12.

[15] Ibid.; p.12.

[16] Ibid.; p.12.

VULNERABILIDADES: son las debilidades, [17]hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por la empresa (amenazas), las cuales se constituyen en fuentes de riesgo.

AMENAZA: es una entidad o agente que puede explotar una vulnerabilidad. Algo o alguien que identificara una vulnerabilidad específica para explotarla y usarla en contra.

RIESGO: es la probabilidad de que un agente, amenaza pueda explotar una vulnerabilidad y el impacto que este tendrá en el negocio.

[17] GAVIRIA ÁLVAREZ, Wilber Arnulfo. Propuesta de actualización de Políticas de Seguridad de la Información del Sistema de Gestión de la Información de la Empresa Caso de Estudio, en la Sede Medellín de la ISO 27001:2005 a la ISO 27001:2013. [En línea].Monografía. Universidad Nacional Abierta y a Distancia UNAD,2017. [Consulta: 12 agosto 2021]. Disponible en: https://repository.unad.edu.co/handle/10596/13274

RESUMEN

La presente propuesta tiene como base el estado actual de las políticas, procesos y procedimientos relacionados con la seguridad de la información de la Universidad Nacional Abierta y a Distancia – UNAD, bajo la norma ISO 27001:2005, (GAVIRIA ALVAREZ, Propuesta de actualización de Políticas de Seguridad de la Información del Sistema de Gestión de la Información de la Empresa Caso de Estudio, en la Sede Medellín de la ISO 27001:2005 a la ISO 27001:2013., 2017),[18] las cuales, permitieron desarrollar el documento, iniciando con una determinación de las fortalezas y debilidades actuales frente a los activos de información, para luego realizar una comparación de estos con lo establecido en la norma ISO 27001:2013.

Esta información permite la proposición de estrategias para la disminución de las vulnerabilidades y la minimización del impacto que pudiera tener la materialización del riesgo en la Universidad. Dando a conocer los controles y políticas que deberían ser implementadas, partiendo de un análisis previo de los activos con los que cuenta actualmente la institución y de esta forma fortalecer el sistema de seguridad de la información, como un proceso de mejora continua que requiere una actualización permanente. Al igual que, algunas recomendaciones para la inclusión de un centro de ciberseguridad CSIRT-UNAD.

Palabras Claves: Controles, información, política, seguridad.

[18] GAVIRIA ÁLVAREZ, Wilber Arnulfo. Propuesta de actualización de Políticas de Seguridad de la Información del Sistema de Gestión de la Información de la Empresa Caso de Estudio, en la Sede Medellín de la ISO 27001:2005 a la ISO 27001:2013. [En línea]. Monografía. Universidad Nacional Abierta y a Distancia UNAD,2017. [Consulta: 12 agosto 2021]. Disponible en: https://repository.unad.edu.co/handle/10596/13274

ABSTRACT

The present proposal is based on the current status of the policies, processes and procedures related to information security of the National Open and Distance University - UNAD, under ISO 27001:2005, (Gaviria Álvarez, 2017), which allowed to develop the document, starting with a determination of the current strengths and weaknesses against the information assets, to then make a comparison of these with the established in the standard ISO 27001:2013.

This information allows the proposal of strategies for the reduction of vulnerabilities and the minimization of the impact that could have the materialización of risk in the University. Making known the controls and policies that should be implemented, based on a prior analysis of the assets currently in the institution and thus strengthen the information security system, as a process of continuous improvement that requires permanent updating. Like, some recommendations for the inclusion of a CSIRT cybersecurity center.

Keywords: Controls, information, policies, security.

1. INTRODUCCIÓN

Tradicionalmente se ha descrito la seguridad de la información, como un conjunto de tres elementos o una triada, que incluye los siguientes conceptos: confidencialidad, integridad y disponibilidad, cada uno de ellos aporta una percepción significativa que permite abarcar la seguridad desde diferentes áreas de trabajo. Es importante mencionar que, se han integrado: la autenticación, para conocer la autoría de las acciones y la información y el no repudio, como la forma de garantizar que algo fue hecho. Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo.

Cada día las organizaciones se enfrentan a demandas en la rentabilidad, la calidad y la seguridad que estimulan el desarrollo sostenible. La norma ISO 27001 ayuda a establecer un Sistema de Gestión de Seguridad de la Información eficiente que permite convertir estas presiones en una ventaja competitiva frente a otras organizaciones del mismo sector.

Por esto es necesario un Centro de Respuestas a Incidentes Informáticos (CSIRT), que ayude al mejoramiento del estado actual de las políticas, procesos y procedimientos relacionados con la seguridad de la información de la Universidad Nacional Abierta y a Distancia UNAD, lo cual conducirá a hacer frente a las grandes problemáticas de seguridad contra la informática que existen, ya que los ataques cibernéticos han evolucionado, implementando nuevas formas de llegar a la información con aplicativos avanzados y sin ningún tipo de apuro por las víctimas, consiguiendo secuestrar, eliminar o modificar la información de una o más personas.

2. PLANTEAMIENTO DEL PROBLEMA

2.1 ANTECEDENTES DEL PROBLEMA

Según [19] En el último año las estadísticas de ataques cibernéticos se han disparado, teniendo en cuenta la pandemia mundial por el covid-19, los nuevos focos de riesgo cibernético generados por la crisis incluyen el trabajo remoto, clases virtuales y las compras en línea, tres tendencias que se aceleraron exponencialmente. Los directores IT y de Seguridad tuvieron que reaccionar tan rápido que dejaron muchas puertas abiertas, usuarios desprotegidos y sitios web mal preparados para el pico en la demanda. Ahora están percibiendo las señales de alarma y, [20]en esta nueva etapa, deberán volver la atención a los detalles de protección de datos, control de identidad y acceso, establecimiento de nuevas políticas de seguridad y revisar su portafolio de aplicaciones con lupa.

Teniendo en cuenta lo anterior, es importante que las organizaciones aumenten la seguridad de sus datos y actualicen de forma constante sus sistemas de gestión, para proteger la red de las amenazas desde su inicio hasta que son confiables y seguras. Según [21]La seguridad de datos es un tema de suma importancia que nos afecta a casi todos nosotros. Cada vez son más los productos tecnológicos que de una u otra forma deben ser tenidos en cuenta para temas de seguridad y que se están introduciendo en nuestra vida cotidiana[22].

La importancia que tiene en las instituciones educativas de incluir una integración de las tecnologías de la información en las universidades que generen importantes impactos positivos en la gestión y operación de las instituciones produciendo eficiencias que a la vez les ayudan a concentrar esfuerzos en su función principal: el aprendizaje. Sin embargo, conforme este proceso de integración avanza, los riesgos asociados a la

[19] ITMASTERSMAG. El estado de la seguridad IT en 2020:[www.itmastersmag.com] Las superficies de ataque se amplían y las personas nunca fueron tan importantes para la defensa[Sitio web],[Consulta: 208 de Octubre de 2020,]Disponnible en: https://itmastersmag.com
[20] Ibid.; p.1.

[21] POWERDATA. www.powerdata.es. [Consulta: el 3 de Diciembre de 2020], de Seguridad de datos: En qué consiste y qué es importante en tu empresa. Disponible en: https://www.powerdata.es/seguridad-de-datos
[22] Ibid.; p.1.

proyección de la información de los estudiantes se hacen también más complejos de atender.[23]

Según [24]el Education Cybersecurity Report 2018, un tercio de los ataques cibernéticos que se realizan actualmente tienen como objetivo a instituciones de educación superior, como ha sido el ataque a inicios del presente año a más de 20 universidades norteamericanas.

De esta forma los CSIRT se han desplazado a lo largo de todo el mundo, estando muy presentes en especial en países con mayor desarrollo tecnológico, quienes se han enfrentados a una serie de ataques informáticos que han conllevado a pérdidas monetarias millonarias y viendo vulnerados sus sistemas[25]. Esto permite que los CSIRT sean reconocidos por crear una red de protección informática para proteger todo el país, cooperando entre ellos para mitigar los riesgos que conlleva cada ataque, en pocas palabras, el país completo está tratando de blindarse por todos los frentes cibernéticos, contando con todos los sectores (educativo, tecnológico, bancario, comercial, etc.)[26].

En este contexto las afectaciones en las instituciones educativas, las cuales, a raíz de la situación de salud presentada, han tenido que duplicar su esfuerzo para atender la demanda de estudiantes con el uso de las Tecnologías de la Información y Comunicación. Aunque algunas universidades ya tenían en su modalidad la Educación a Distancia como su enfoque principal, se han visto perjudicadas por la cantidad de ataques que vienen en aumento[27]. Por esto, es necesario plantear un Centro de Respuestas a Incidentes Informáticos (CSIRT), que ayude al mejoramiento del estado actual de las políticas, procesos y procedimientos relacionados con la seguridad de la información en la Universidad Nacional Abierta y a Distancia UNAD

[23] SECURITYSCORECARD. www.securityscorecard.com. [Consulta: en 2018], de Informe sobre ciberseguridad en la educación 2018. Disponible en: https://securityscorecard.com/resources/2018-education-report
[24] Ibid.; p.1.

[25] CANO VARGAS, J., [En línea], [Consulta: en 2020]. Propuesta de los documentos administrativos para la Creación de un Centro de Respuesta a Incidentes Cibernéticos para la empresa caso de estudio Cibersecurity de Colombia LTDA. Disponible en. https://repository.unad.edu.co/bitstream/handle/10596/36488/jjcanov.pdf?sequence=1&isAllowed=y
[26] Ibid.; p.26.
[27] Ibid.; p.29.

2.2 FORMULACIÓN DEL PROBLEMA

Debido a la modalidad de educación abierta y a distancia implementada por la UNAD[28], día a día está expuesta a los crecientes ataques cibernéticos y la sofisticación de estos, los cuales pueden infringir los controles establecidos por la universidad, dejando vulnerable el acceso a los sistemas de información y exponiendo los mismos a perdida, modificación y uso inadecuado de la información allí almacenada.[29]
La universidad cuenta con la matriz de riesgos de seguridad de la información la cual es actualizada anualmente, pero no se realiza la actualización oportuna de la declaración de aplicabilidad[30], por lo cual no se tiene claramente identificadas, organizadas y registradas las medidas de seguridad implementadas y las exclusiones o adopciones de controles de seguridad de los activos de la información.[31]

Adicionalmente, no se cuenta con un equipo de seguridad [32] de la información dedicado a la ejecución de actividades específicas en este campo de acción, tales como: desarrollo, mantenimiento y seguimiento al marco normativo referente a seguridad de la información, identificación de stackeholders, análisis y tratamiento de los riesgos de seguridad a los cuales puede estar expuesta la universidad, gestión, análisis, registro y gestión de incidencias, definición y seguimiento a indicadores.[33]

La UNAD tiene establecidos lineamientos y controles de seguridad de la información, que permiten mantener la integridad, disponibilidad y confidencialidad de la información institucional [34] , sin embargo, se debe realizar seguimiento al cumplimiento de las políticas definidas y alinearlas entre si conforme a las exigencias del gobierno y las institucionales.

---

[28] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA[Sitio web]. [gidt.unad.edu.co] Seguridad de la información Principios básicos de Seguridad Informática y de la Información. [Consulta: en 2020], Disponible en. https://gidt.unad.edu.co/seguridad-de-la-informacion
[29] Ibid.; p.1.

[30] UNIVERSIDD NACIONAL ABIERTA Y A DISTANCIA [U.N.A.D]. (Consulta: 2 de Febrero de 2018). Plan Estratégico de Seguridad y Privacidad de la Información GIDT-PTI. Disponible en: https://gidt.unad.edu.co/images/Documentos/Plan-de-Seguridad-y-Privacidad-de-la-Informacion.pdf
[31] Ibid.; p.9.
[32] Ibid.; p.9.
[33] Ibid.; p.7.
[34] Ibid.; p.10.

Teniendo en cuenta lo anterior surge el siguiente interrogante:

¿Cómo mejorar el estado actual de las políticas, procesos y procedimientos relacionados con la seguridad de la información de la Universidad Nacional Abierta y a Distancia UNAD, con un Centro de Respuestas a Incidentes Informáticos (CSIRT)?

3. JUSTIFICACIÓN

La Universidad Nacional Abierta y a Distancia (UNAD) tiene como misión contribuir a la educación para todos a través de la modalidad virtual asequible y en ambientes virtuales de aprendizaje, apoyándose en las tecnologías de la información y las comunicaciones, para fomentar y acompañar una formación autónoma de los estudiantes. Para ello tiene establecida una normativa de lineamientos y controles de seguridad de la información, que permiten fortalecer la autenticación, integridad, disponibilidad y confidencialidad de la información institucional. Siendo una de las universidades más grandes en el territorio nacional, con un amplio número de estudiantes matriculados en los programas académicos en conjunto de una infraestructura tecnológica robusta que permite gestionar y almacenar grandes volúmenes de información del personal, bien sea administrativo, de docencia y, estudiantil, esta debe velar por mantener segura y protegida la información que administra. Por lo anterior, es preciso dar una mirada a las políticas, procesos y procedimientos relacionados con la seguridad de la información que se encuentran actualmente implementados, con el fin de contribuir en el fortalecimiento de estos. De esta forma se operará el sistema de manera planificada para minimizar el impacto que pueda generar un incidente de seguridad materializado, solucionando oportunamente este tipo de eventualidades, para así dar evidencia del cumplimiento a la aceptación del riesgo definido por la Universidad.
Así mismo, adicional a la verificación del sistema de gestión de la seguridad de la información, es importante incluir desde el nivel directo algunas recomendaciones para Centro de Respuestas a Incidentes Informáticos (CSIRT).

Estos lineamientos deben estar acordes a los objetivos y planes estratégicos de TI institucionales, los cuales permitirán actuar de manera acertada ante una eventualidad, minimizando los periodos de indisponibilidad de los servicios y fortaleciendo la seguridad de los activos de la información críticos para la UNAD.

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Diseñar un esquema de ciberseguridad para el Centro de Respuestas a Incidentes Informáticos CSIRT, que apoye al mejoramiento del estado actual de las políticas, procesos y procedimientos relacionados con la seguridad de la información de la Universidad Nacional Abierta y a Distancia – UNAD

4.2 OBJETIVOS ESPECÍFICOS

1. Enunciar la estructura de la Universidad, roles, responsabilidades y funciones relacionadas con el área de tecnologías de la información y la respuesta a incidentes informáticos.

2. Documentar el estado actual Universidad acerca de las políticas, procesos y procedimientos.

3. Proponer la organización, roles, responsabilidades y funciones del centro de respuesta a incidentes informáticos CSIRT-UNAD.

4. Formular un plan estratégico para la atención de eventos cibernéticos en coordinación con el área de TI, que incluya políticas y procedimientos de actuación.

5. MARCO REFERENCIAL

5.1 MARCO TEÓRICO

La transformación tecnológica ha obligado a todos los sectores a evolucionar a estados ampliamente marcados por tendencias de expansión y cobertura, y el sector educación no ha sido la excepción, tal como lo menciona la UNESCO[35] en el informe *La educación superior en el sigo XXI* indica: La necesaria evolución de la educación superior como espacio de formación, al que se podrá acceder con una gran flexibilidad en cualquier edad para una formación intensiva o para la actualización de los conocimientos y la adquisición de nuevas competencias o para fines de reconversión, constituye uno de los aspectos principales de la democratización y la renovación de la educación superior y de la educación en general.

A través del uso de las tecnologías de la información y de las comunicaciones se ha venido modificando la forma de crear contenidos, adquirir y transmitir el conocimiento a un público especifico a través de espacios virtuales de aprendizaje, y ante la creciente demanda de la adquisición de conocimiento a través de la modalidad de educación a distancia, las universidades deben implementar nuevas tecnologías, fortalecer los niveles de seguridad de los activos de la información, políticas y lineamientos de seguridad más robustos aplicados a los nuevos entornos y recurso humano preparado para afrontar de manera oportuna los riesgos y amenazas de ciberseguridad a los que se está expuestos, permitiendo garantizar la continuidad del servicio y la seguridad de la información administrada por los diferentes sistemas de información.

En la actualidad el acceso a internet ha venido en aumento con diferentes intensiones por parte de los consumidores, y según el análisis de Índice de Apropiación Digital en Colombia realizado por el Centro de Nacional de Consultoría, este índice en Colombia es del 0,24 por encima de países de América como México, Chile y Argentina. Por encima de ese promedio nacional, están aquellas personas que participan de procesos

[35] UNESCO.Declaración mundial sobre la educacion superior en el siglo XXI: Visión y Acción[www.iesalc.unesco.org] [Consulta: el 20 de Agosto de 2019], Disponible en: https://www.iesalc.unesco.org/ess/index.php/ess3/article/view/171

educativos virtuales (0,46), los que ejercen algún tipo de activismo por medios virtuales (0,46), los que hacen gran parte de sus compras por Internet (0,47) y aquellos que realizan transacciones bancarias (0,51). Como resultado del estudio, también se evidenció que el uso de las herramientas digitales en mayor medida se da para fines de entretenimiento, comunicación básica, y en porcentajes menores en procesos educativos, transacciones virtuales, y transformación digital para emprendimientos en búsqueda de incremento de ingresos[36]

Con el incremento en el uso de las plataformas digitales para realizar diferentes tipos de procesos e intercambio de información, también crecen exponencialmente los volúmenes de información almacenadas en las bases de datos para su procesamiento, y con ellos los ciberataques los cuales exponen la misma para obtener acceso no autorizado con fines maliciosos. Según la Asobancaria, el panorama de riesgos cibernéticos indica que 4 de cada 10 organizaciones han sufrido una brecha de seguridad en los últimos 24 meses con respecto al 2016, en el 2017 se registraron aproximadamente 677 millones de amenazas cibernéticas en América Latina (Asobancaria, 2017), y de acuerdo con el informe Balance del Cibercrimen realizado por el Centro Cibernético Policial, en Colombia para el 2017 los delitos informáticos aumentaron en un 28,3% frente al 2016.

Según el estudio realizado por la empresa consultora EY, el 87% de las organizaciones operan con niveles limitados de ciberseguridad y resiliencia, mientras que el 77% trabaja con medidas de protección básicas en materia de ciberseguridad y buscan mejorar sus capacidades haciendo uso de tecnologías avanzadas como inteligencia artificial, automatización robótica de procesos y analítica de datos, entre otras.

Según el estudio de Tendencias del Cibercrimen 2019-2020[37], presentado por el Tanque de Análisis y Creatividad de las TIC - Tictac de la CCIT y su programa SAFE en asocio con la Policía Nacional - Centro Cibernético Policial, se evidencia que la dinámica actual del cibercrimen en Colombia refleja un crecimiento gradual en el número de incidentes

[36] UNESCO. Declaración mundial sobre la educacion superior en el siglo XXI: Visión y Acción[www.iesalc.unesco.org] [Consulta: el 20 de Agosto de 2019], Disponible en: https://www.iesalc.unesco.org/ess/index.php/ess3/article/view/171

[37] TELECOMUNICACIONES. CCTI Camara Colombiana de Informatica y. [Consulta: en Octubre de 2019] Obtenido de Tendencias del Cibercrimen en Colombia 2019-2020: Disponible en: https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

cibernéticos reportados a las autoridades del ecosistema de ciberseguridad. A través de los canales dispuestos por la Policía Nacional fueron registrados 28.827 casos de incidentes cibernéticos durante el 2019, frente a 22.524 reportados en el 2018 y 15.840 en el 2017. Los incidentes más reportados en Colombia son los casos de Phishing con un 42%, suplantación de Identidad 28%, el envío de malware 14% y los fraudes en medios de pago en línea con 16%.[38]

El cibercrimen en América Latina y el Caribe han costado alrededor de US$90.000 millones al año correspondiente al 16% del costo total mundial reportado por este delito (CAI Virtual, 2017), según Luis Garzón administrador de cuentas de seguridad CISCO indica que el ciber fraude en Colombia está generando pérdidas por 1 billón de pesos.

Primer ejemplar de Malware auto replicable, en la historia de la ciberseguridad, conocido entonces como el Gusano Morris[39] en (1988), el cual afecto a la internet el 2 de noviembre de 1988, siendo este el primer gusano informático. Morris worm durante unas horas aproximadamente el 10% de las todas las maquinas conectadas a internet se vieron afectadas por ese gusano. Es de allí que el mundo se ve en la necesidad de cooperar y coordinarse entre los administradores de los sistemas y gestores de IT para mitigar e investigar este tipo de casos.

Algunos días después del caso Morris, la DARPA (Defence Advanced Research Projects Agency-Agencia de Investigación de Proyectos Avanzados de defensa) crea entonces el primer CSIRT, llamado CERT/CC, ubicado este en la universidad de Carnegie Mellon, en Pittsburgh (Pensilvania).

[38] TELECOMUNICACIONES. CCTI Camara Colombiana de Informatica y. [Consulta: en Octubre de 2019] Obtenido de Tendencias del Cibercrimen en Colombia 2019-2020: Disponible en: https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

[39] PERIODISTA DIGITAL. El Gusano Morris y los daños que causó en Internet [Sitio web], [Consulta: 16 de julio de 2019]. Disponible en:https://www.periodistadigital.com/tecnologia/tec-internet/20190726/gusano-morris-danos-causo-internet-noticia-689404036001/

5.2 MARCO CONCEPTUAL

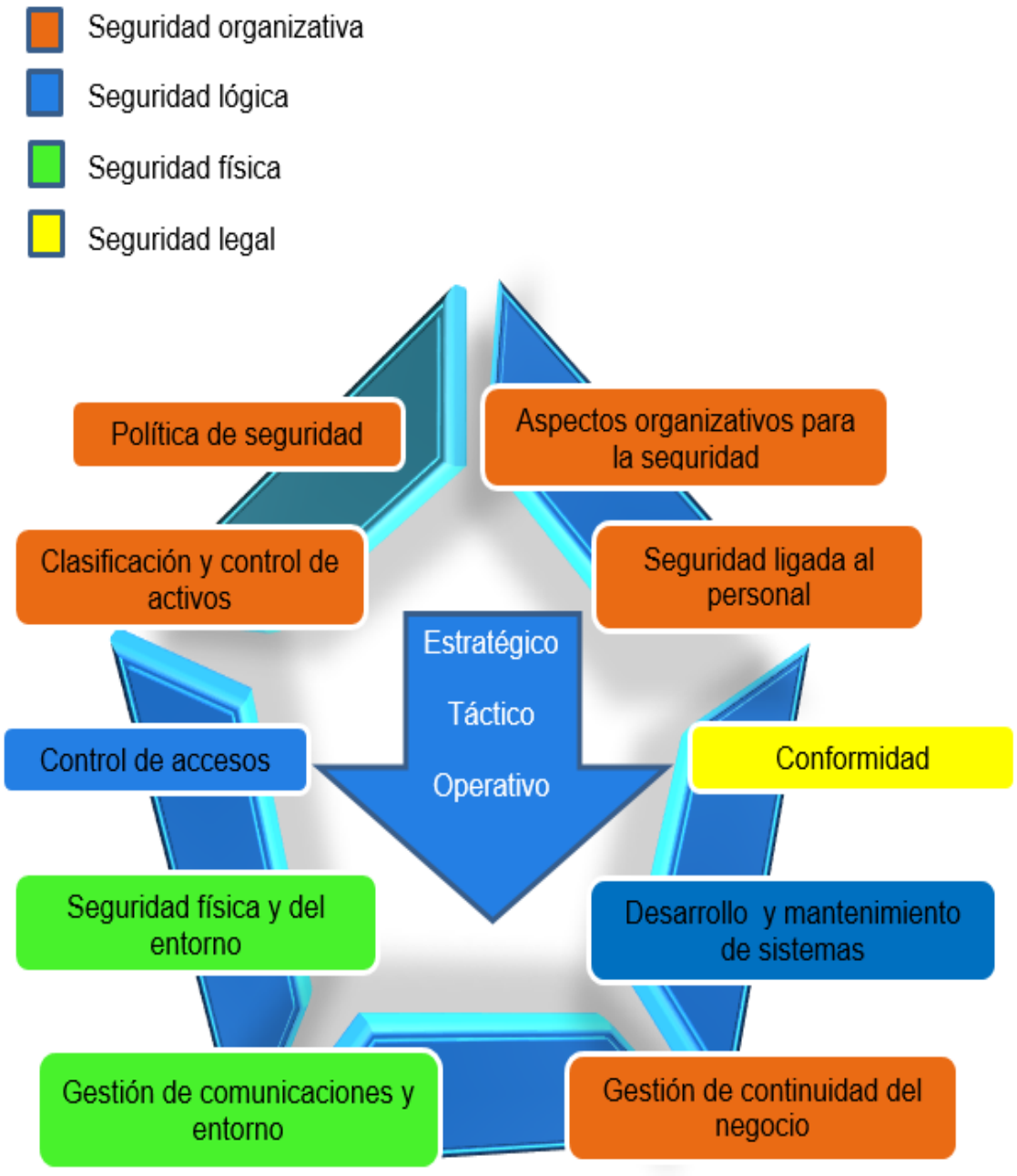
5.2.1 SEGURIDAD DE LA INFORMACIÓN

Es la protección de la información que hay en una entidad o que un individuo maneja. Esta información representa un activo valioso para la organización.
La información ahora está expuesta a un número cada vez mayor y una variedad más amplia de amenazas y vulnerabilidades (véase también OECD Guía para la seguridad redes sistemas de información). Según la ISO/IEC 17799[40] 6, la información puede existir en muchas formas. Puede estar impresa o escrita en un papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, mostrada en películas o hablada en una conversación. Cualquiera que sea la forma que tome la información, o medio por el cual sea almacenada o compartida, siempre debiera estar apropiadamente protegida.

la seguridad de la información se alcanza implementando un conjunto adecuado de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Se necesita establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de seguridad y comerciales específicos. Esto se debiera realizar en conjunción con otros procesos de gestión del negocio.

[40] SLIDESERVER. Gestión de la Seguridad de la Información según ISO/IEC 17799.[www.slideserve.com] [Consulta: 11 de Nov de 2012] Disponible en: https://www.slideserve.com/yoshiko/gesti-n-de-la-seguridad-de-la-informaci-n-seg-n-iso

Figura 1. Gestión de la Seguridad de la Información según ISO/IEC 17799[41]



Fuente 1 Elaboración Propia

[41] SLIDESERVER. Gestión de la Seguridad de la Información según ISO/IEC 17799.[www.slideserve.com] [Consulta: 11 de Nov de 2012] Disponible en: https://www.slideserve.com/yoshiko/gesti-n-de-la-seguridad-de-la-informaci-n-seg-n-iso

5.2.2 SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Un Sistema de Gestión de la Seguridad de la Información (SGSI) es una herramienta que sirve de ayuda a las diferentes empresas, para implementar políticas, procedimientos y controles de seguridad informática acordes con los objetivos del negocio.

Teniendo en cuenta el concepto establecido en la norma ISO 27001:20058, este es parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.[42]

Figura 2. Principios de la seguridad informática: Confidencialidad, Integridad y Disponibilidad de la información.

Fuente 2 Elaboración Propia

[42] LISOT. Principios de la seguridad informática: Confidencialidad, Integridad y Disponibilidad de la información. [www.lisot.com] [Consulta: en 2021] Disponible en. Obtenido de https://www.lisot.com/que-es-un-sistema-de-gestion-de-la-seguridad-de-la-informacion-sgsi/

5.2.3 FAMILIAS DE LAS NORMAS ISO/IEC 27000

Es un conjunto de normas de gestión de la seguridad de la información con la IEC (International Electrotechnical Commission), comisión internacional de electrotecnia, tiene algunas similitudes a la familia de las normas de gestión de la calidad ISO 9000. Cada una de las normas de la familia 270009, define y centra todos los aspectos importantes en el contexto de la gestión de la seguridad de la información en cualquier empresa pequeña, mediana o grande, así como públicas y privadas.[43]

Cuadro 1. ISO 27000 la familia de normas.[44]

Fuente 3 Elaboración Propia

[43]ISOTOOLS. La familia de normas ISO 27000.[www.isotools.org][Sitio web]Esta estandarización contiene las definiciones y los términos que se utilizarán durante toda la serie 27000.[Consulta: 21 de Enero de 2015] Disponible en:https://www.isotools.org/2015/01/21/familia-normas-iso-27000/

[44] Ibid.; p.1.

5.2.4 QUE SIGNIFICA Y QUE ES UN CSIRT.?

Un **CSIRT** como sus siglas lo indican **Computer Security Incidente Response Team** o el Equipo de respuestas a incidentes de seguridad informática.

Es un grupo o equipo de personas que están especializados en seguridad informática y que estos ejecutan, coordinan y se apoyan para dar respuesta a los incidentes de ciberseguridad que ocurren en alguna entidad, esto con el objetivo de ayudar a minimizar y controlar el impacto o daño que resulte en un incidente informático y se pueda recuperar de un ataque.

5.2.5 TIPOS DE CSIRT.

- CSIRT del sector Académico
- CSIRT comercial
- CSIRT del sector Publico
- CSIRT interno
- CSIRT del sector militar
- CSIRT nacional
- CSIRT del soporte - PSIRT

5.2.6 CSIRT DEL SECTOR ACADÉMICO.

Estos servicios son prestados en las organizaciones de educación y en las comunidades académicas; tales como las universidades, colegios, escuelas, centros de formación, y también a institutos de investigación y a sus Campus Virtuales. En el CSIRT[45], Determinar el tamaño de las instalaciones puede variar debido a la comunidad que se le va a prestar el servicio o que se va a atender, esto puede estar sujeto a una facultad, una institución, una sede universitaria, o a los centros, grupos e instituciones de investigación. En ocasiones estos equipos de respuesta a incidentes, integran sus esfuerzos con otros CSIRT y de ellos algunas se especializan en algunas investigaciones.

[45] GILLERMON BENITEZ RODRIGUEZ. Diseño documental para creación de un CSIRT. [En línea]. Monografía. Universidad Nacional Abierta y a Distancia UNAD,2020. [Consulta: 26 marzo 2020]. Disponible en: ttps://repository.unad.edu.co/bitstream/handle/10596/36672/gmbenitezr.pdf?sequence=1&isAllowed=y

5.3 MARCO HISTÓRICO

5.3.1 POLÍTICAS: EN ESTE SEGMENTO SE OBSERVARÁN ALGUNAS POLÍTICAS ANTERIORMENTE RELACIONADAS CON LA INVESTIGACIÓN SOBRE LAS POLÍTICAS.

5.3.2 GAVIRIA ÁLVAREZ, WILBER ARNULFO 2017-09-27.

propuesta de actualización de políticas de seguridad de la información del sistema de gestión de la información de la empresa caso de estudio, en la sede Medellín de la iso 27001:2005 a la iso 27001:2013.

Resumen: en la presente propuesta de actualización de los controles y las políticas de seguridad de la información, se tomó como base el estado actual de lo ya dispuesto en la empresa caso de estudio bajo la norma iso 27001:2005, lo que nos permitió determinar las fortalezas y debilidades que se tienen frente a los activos de información, realizando la comparación de estos con lo establecido en la norma iso 27001:2013, información que nos ayuda a generar estrategias que minimizan las amenazas que puedan impactar las vulnerabilidades de la organización, dando a conocer los controles y políticas que deben ser implementadas, las cuales son producto del análisis de lo que posee implementado la empresa en mención, lo que aportara al fortalecimiento del sistema de seguridad de la información de la organización, como un proceso de mejora continua que requiere la actualización permanente.[46]

5.3.3 OCHOA CASTAÑEDA, JAIME ANDRES; VELA FORIGUA, LINA MARÍA 2018-04-01.

Creación de políticas de seguridad para Cormagdalena.

Resumen: Este trabajo trata de como ayudaremos con esta investigación que realizamos a la empresa Cormagdalena a implementar un excelente esquema de políticas de seguridad, ya que por ser una empresa del estado cuenta con muchas falencias en sus políticas de seguridad por el ahorro de costos, es así como llegamos a visualizar en esta investigación que la mayoría de compañías por el avanzan sin límites de la tecnología, las empresas asumen riesgos como perder un negocio o

[46] GAVIRIA ÁLVAREZ, Wilber Arnulfo. Propuesta de actualización de Políticas de Seguridad de la Información del Sistema de Gestión de la Información de la Empresa Caso de Estudio, en la Sede Medellín de la ISO 27001:2005 a la ISO 27001:2013. [En línea].Monografía. Universidad Nacional Abierta y a Distancia UNAD,2017. [Consulta: 12 agosto 2021]. Disponible en: https://repository.unad.edu.co/handle/10596/13274

arriesgarse a ser hackeadas; en ocasiones estas políticas de seguridad son utilizadas incorrectamente provocando daños de grandes dimensiones. Se realiza esta investigación para explicar el proceso de creación de políticas de seguridad de la información para la empresa Cormagdalena y adicional poder dejar una guía para todo aquel que lea este trabajo pueda tener una serie de indicadores para la realización de futuros proyectos de investigación. Queremos con lo investigado y plasmado aquí que las personas vean la seguridad de la información como algo muy importante en el proceso y desarrollo de las compañías y no como una parte incómoda para la alta gerencia o un obstáculo para el crecimiento como algunos lo ven, más bien insistir en que si se realiza una excelente política de seguridad la compañía va a tener un crecimiento asegurado y con excelente calidad.[47]

5.3.4 JOHN JAIRO LEIVA JIMÉNEZ JUAN CARLOS CHIARI CABALLERO-2012-11-23.

Implementación de la fase inicial de un sistema de gestión de la seguridad de la información en el grupo de TI de una entidad del sector público colombiano.

Resumen: este trabajo trata de como ayudaremos con esta[48] investigación que realizamos a la empresa cormagdalena a implementar un excelente esquema de políticas de seguridad, ya que por ser una empresa del estado cuenta con muchas falencias en sus políticas de seguridad por el ahorro de costos, es así como llegamos a visualizar en esta investigación que la mayoría de compañías por el avanzan sin límites de la tecnología, las empresas asumen riesgos como perder un negocio o arriesgarse a ser hackeadas; en ocasiones estas políticas de seguridad son utilizadas incorrectamente provocando daños de grandes dimensiones. se realiza esta investigación para explicar el proceso de creación de políticas de seguridad de la información para la empresa cormagdalena y adicional poder dejar una guía para todo aquel que lea este trabajo pueda tener una serie de indicadores para la realización de futuros proyectos de investigación. queremos con lo investigado y plasmado aquí que las personas vean la seguridad de la información como algo muy importante en el proceso y desarrollo de las compañías y no como una parte incómoda para la alta

[47] OCHOA CASTAÑEDA, Jaime Andres. Propuesta de la Creación de políticas de seguridad para Cormagdalena. [En línea]. Monografía. Politécnico grancolombiano [Consulta: 7 mayo 2018]. Disponible en: https://alejandria.poligran.edu.co/handle/10823/1227

[48] LEIVA JIMENEZ, John Jairo., y CHIARI CABALLERO, Juan Carlos. Implementación de la fase inicial de un sistema de gestion de la seguridad de la información en el grupo de TI de una entidad del sector publico colombiano. [En línea]. Monografía. Universidad Piloto de Colombia [Consulta: 12 agosto 2013]. Disponible en http://polux.unipiloto.edu.co:8080/00001038.pdf

gerencia o un obstáculo para el crecimiento como algunos lo ven, más bien insistir en que si se realiza una excelente política de seguridad la compañía va a tener un crecimiento asegurado y con excelente calidad.

5.4 MARCO LEGAL

Estándares para la seguridad de la información[49]

ISO/IEC 27001 Sistema de gestión de seguridad de la información - SGSI. Define los requerimientos para establecer y gestionar un SGSI.

ISO/IEC 27002 Conjunto de buenas prácticas para la implantación del SGSI, a través de 114 controles, estructurados en 14 dominios y 35 objetivos de controles.

ISO/IEC 27014 Gobernanza de seguridad de la información

NIST (National Institute of Standards and Technology)

Ley 1341 del 30 DE JULIO DE 2009 Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC

Ley 1581 de 2012 del 17 de octubre del 2012 Protección de datos personales

Estrategia de gobierno digital

CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.

CONPES 3854 de 2016. Política Nacional de Seguridad digital.

[49] ISOTOOLS. La familia de normas ISO 27000.[www.isotools.org][Sitio web]Esta estandarización contiene las definiciones y los términos que se utilizarán durante toda la serie 27000.[Consulta: 21 de Enero de 2015] Disponible en:https://www.isotools.org/2015/01/21/familia-normas-iso-27000/

6. DISEÑO METODOLÓGICO

Este documento se diseñará a través del tipo de investigación aplicada, pues esta forma de estudio utiliza métodos, teorías y conocimiento históricos para ser aprovechados en la actualización de las políticas de seguridad de la información, para minimizar los efectos causados por los delitos informáticos, quienes atacan directamente los activos ya sean personales o de una agrupación legalmente constituida como lo es la Universidad Nacional Abierta y a Distancia UNAD. Para aumentar la protección a los datos de los usuarios que navegan en la plataforma de la universidad en conjunto con la implementación de Centro de Respuestas a Incidentes Informáticos CSIRT.

Fuente de información

Se recopilará información y parámetros procedimentales de las políticas que están regidas en la plataforma de la UNAD, permitiendo hacer un análisis más detallado para determinar en cuál de estas debe realizarse una actualización que nos permita detectar nuevas problemáticas que se están viviendo en nuestros días referente a un aumento de ciberataques por la crisis del COVID-19, que provocó un crecimiento exponencial de los espacios educativos virtuales, en conjunto con la ciberdelincuencia.

Recolección de información

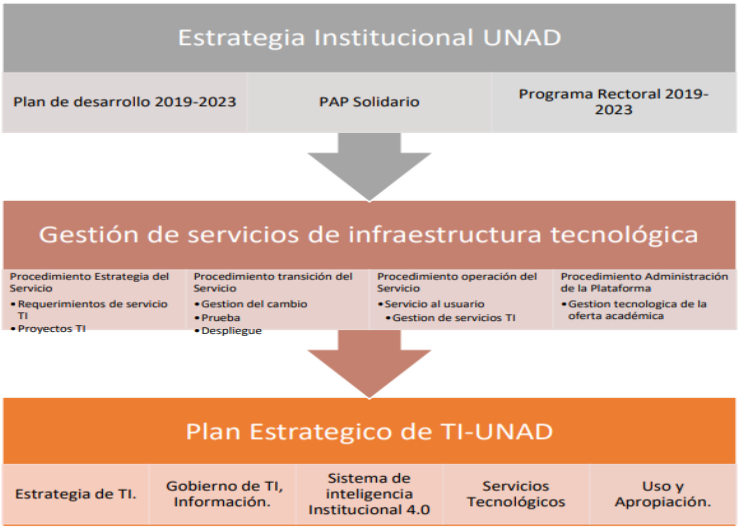
La información necesaria para la propuesta se conseguirá por medio de encuestas, utilizando un grupo especifico de estudiantes que interactúan con la plataforma educativa, donde se obtendrán datos sobre experiencias, conocimiento y problemas informáticos vigentes, por medio de preguntas cerradas o de selección múltiple, así se podrá crear una estadística que apoya la estructura del proyecto.

7. ESTRUCTURA DEL ÁREA DE TECNOLOGÍA DE LA UNIVERSIDAD UNAD.

La UNAD actualmente cuenta con una variedad de sistemas de información tanto desarrollados internamente como adquiridos, los cuales se han implementado para satisfacer necesidades puntuales de información y gestión. Dentro del PLAN RECTORAL 2019 -2023 se expone la utilización de infotecnologias, el Blockchain, machine Learning entre otros, como parte del Sistema de Inteligencia Institucional (SII UNAD 4.0). Dispositivo que permite gestionar altos flujos de información, en cada uno de los sistemas, unidades y redes integrantes del meta sistema UNAD, como insumos para el análisis que precede a la toma de decisiones. La utilización del SII 4.0 generará transparencia, efectividad y rigor en la gestión integral individual y colectiva de la universidad y permitirá afianzar las interrelaciones internas y externas de la organización aplicando de manera rigurosa sus propios estándares, en concordancia con los provenientes del nivel nacional e internacional.

Para este primer objetivo se logrará evidenciar el organigrama de la universidad específicamente la del área de tecnología en relación a la seguridad de la información y de cómo se da respuesta a las incidencias que se presenten, debido a la importancia de esta gestión en una universidad centrada en el aprendizaje virtual.[50]

Figura 3. Estrategia de TI de la UNAD



Fuente 4 Elaboración Propia

[50] UNIVERSIDD NACIONAL ABIERTA Y A DISTANCIA [U.N.A.D]. Plan Estratégico de Seguridad y Privacidad de la Información GIDT-PTI.[sitio web] [Consulta: 2 de febrero de 2018] Disponible en: https://gidt.unad.edu.co/images/Documentos/Plan-de-Seguridad-y-Privacidad-de-la-Informacion.pdf

Gestión de la Información

La UNAD cuenta con diferentes sistemas y fuentes de información, los cuales están bajo la responsabilidad de las unidades que los operan dentro del Plan de Desarrollo 2019-2023 “Más UNAD, más PAÍS” , dentro de la institución las unidades encargadas de la Gestión tecnológica son la Vicerrectoría de Innovación y Emprendimiento como componente estructural del meta sistema UNAD de carácter misional, encargado de brindar lineamientos que potencien la vanguardia tecnológica de la UNAD y Gerencia Plataformas e Infraestructuras Tecnológicas, componente estructural del Meta sistema UNAD, de carácter funcional, responsable de gestionar las plataformas, recursos tecnológicos, sistemas y servicios de información digital para las unidades y miembros de la comunidad universitaria, con sentido de eficiencia, calidad, seguridad integral, productividad y competitividad.

Funciones de la Gerencia de Plataformas e Infraestructuras Tecnológicas.

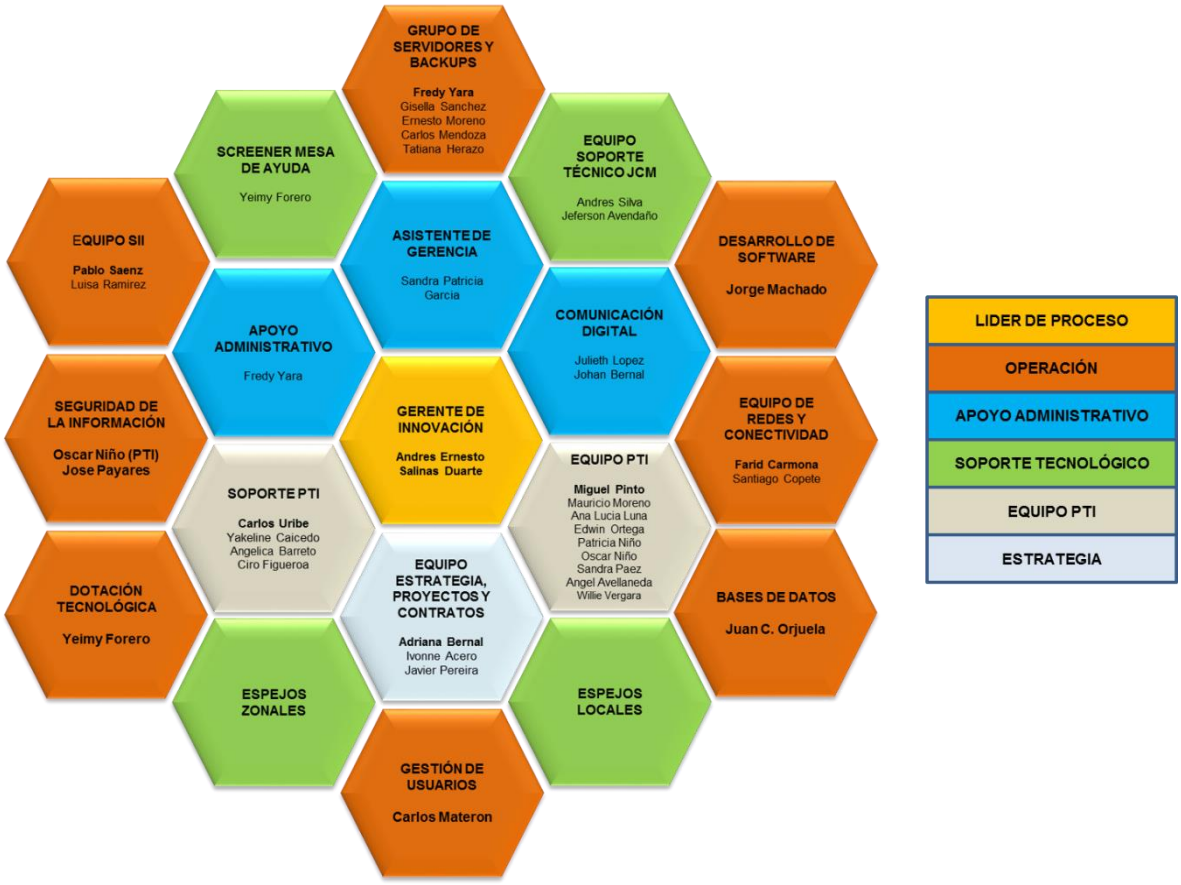
Tabla 1. Esta unidad cumplirá las siguientes funciones:

LITERAL	FUNCIONES
LITERAL G:	Propender por el uso racional, la optimización y la seguridad informática y de la información institucional de la Universidad
LITERAL I:	Evaluar las condiciones técnicas de los recursos tecnológicos de la Universidad con el fin de propender por la seguridad, funcionamiento y continuidad de la operación.
LITERAL J:	Cumplir con los procesos y procedimientos derivados de SIG UNAD, a fin de que todas las acciones y decisiones bajo su responsabilidad queden inmersas y a la vista de todos aquellos usuarios y beneficiarios internos y externos.
LITERAL M:	Administrar el componente técnico para la integración de la información institucional de manera integral garantizando su seguridad, confiabilidad, precisión y actualidad.
LITERAL N:	Evaluar las condiciones técnicas de los recursos tecnológicos de la Universidad y realizar su mantenimiento y actualización de manera preventiva y correctiva.
LITERAL P:	Coordinar y desarrollar, en conjunto con las unidades del sistema misional, asesorías, consultorías, interventorías y asistencia técnica relacionada con su campo de acción.
LITERAL Q:	Coordinar, con las demás unidades, los planes, programas y proyectos necesarios para el cumplimiento de sus funciones.
LITERAL T:	Desarrollar el proceso de mejora continua de los procedimientos, instrumentos y herramientas que lidera dentro de los procesos del Sistema Integrado de gestión

A continuación, puede consultar la organización del equipo de la Gerencia de Innovación y Desarrollo Tecnológico, el cual se compone de:[51]

- Líder de proceso
- Operación
- Apoyo administrativo
- Soporte tecnológico
- Equipo de Plataforma Tecnológica Integrada - PTI
- Estrategia

Figura 4. Organigrama Equipo Tecnología Integrada – PTI UNAD.



Fuente 5 Elaboración Propia

[51] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. (2021). Gerencia de Innovación y Desarrollo Tecnológico Organigrama PTI [Sitio web] [Consulta: en el 2020]. Disponible en:https://gidt.unad.edu.co/acerca-de/organigrama

Tabla 2. Roles y responsabilidades área tecnologías de la información[52].

ROL	RESPONSABILIDADES
Líder de proceso	Planear, administrar y suministrar la infraestructura tecnológica de la UNAD, asegurando la disponibilidad de los servicios de Tecnologías de la Información requeridos por los Procesos Misionales, Estratégicos, de Apoyo y Evaluación, para el cumplimiento de los objetivos institucionales. ✓ Gestionar los recursos tecnológicos al servicio de las unidades y miembros de la comunidad universitaria. ✓ Evaluar las condiciones técnicas de los recursos tecnológicos de la universidad y realizar su mantenimiento y actualización de manera preventiva y correctiva ✓ Evaluar y proponer la incorporación planificada de nuevas y mejores tecnologías para la universidad. ✓ Gestionar la conectividad y soporte de infraestructura telemática, a todos los procesos académicos, financieros y administrativos. ✓ Garantizar la calidad, el uso racional, la optimización y la seguridad de las tecnologías de la información y las comunicaciones, en la universidad. ✓ Diseñar estrategias innovativas para la gestión y aplicación de recursos tecnológicos, que garanticen la sostenibilidad técnica, para el desarrollo de los procesos de formación a distancia en línea, mediante la utilización de tecnologías telemáticas. ✓ Impulsar y garantizar la calidad de sus servicios mediante el desarrollo eficiente y efectivo de las acciones técnicas basadas en los criterios de actuación de la universidad. ✓ Administrar tecnológicamente el sistema integrado de información institucional en sus diferentes componentes, académico, financiero y administrativo y garantizar su seguridad, confiabilidad, precisión y actualidad. ✓ Coordinar, con las demás unidades, los planes, programas y proyectos necesarios para el cumplimiento de sus funciones Las demás que, por su naturaleza, establezca la Rectoría.
Soporte tecnológico	El equipo de trabajo de Soporte Técnico está dedicado a responder con eficiencia y veracidad a los incidentes y requerimientos tecnológicos reportados por el usuario interno de la UNAD a través de la aplicación Mesa de Ayuda, con el fin de mantener y mejorar la disponibilidad de las herramientas tecnológicas utilizadas por el personal para el desarrollo de sus labores diarias. Para la atención, el equipo de Soporte Técnico de la GIDT mantiene unos Acuerdos de Nivel de Servicio (ANS) con los cuales se comprometen a atender a las solicitudes en un tiempo máximo definido, a partir de la apertura del ticket, así: INCIDENTE: 1.440 minutos (3 Días hábiles) REQUERIMIENTOS: 3.840 minutos (8 Días hábiles)
Equipo de Plataforma Tecnológica Integrada - PTI	Administrar las subplataformas brindando el apoyo técnico necesario para gestionar las actividades en campus y realizar el respaldo de los cursos académicos al finalizar los periodos, como medida de aseguramiento de la integridad y disponibilidad de la información.

[52] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. (2021). Gerencia de Innovación y Desarrollo Tecnológico Organigrama PTI [Sitio web] [Consulta: en el 2020]. Disponible en: https://gidt.unad.edu.co/acerca-de/organigrama

	Gestionar, administrar y realizar seguimiento al conjunto de subplataformas que conforman el campus virtual, optimizando los recursos y manteniendo la adecuada prestación de los servicios académicos y administrativos.

7.1 POLÍTICAS PROCESOS Y PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA UNAD.

Frente a la responsabilidad que posee la universidad UNAD, al garantizar una educación virtual, la información que se proporciona en las plataformas para satisfacer su creciente demanda educativa, debe cumplir con una normativa que gestione y administre la seguridad de la misma. Inicialmente es necesario el reconocimiento de las políticas, procesos y procedimientos demuestran una implementación, operación, seguimiento, revisión, mantenimiento y mejora del Sistema de Gestión de la Seguridad de la Información (SGSI) basada en la norma IS027001:2013. En mérito de lo expuesto, se comprende las políticas y procedimientos de seguridad de la información en la universidad, en puntos estratégicos que se relacionan con el tema central del proyecto de investigación.

A continuación, en la siguiente tabla, se segmenta la información que menciona los capítulos y artículos que componen el apartado completo de la administración y gestión de la seguridad para garantizar la protección de la información dentro del plantel educativo que está en la misma línea con el objetivo del trabajo de grado en cuestión.

Tabla 3. Políticas Actuales En la UNAD.

CAPÍTULOS	ARTÍCULOS
CAPÍTULO I: Disposiciones generales.	**Artículos:** 1, 2, 3. Apoyo de implementación del Sistema de Gestión de Seguridad, aplicando las diferentes definiciones para adoptar la resolución en funcionarios y administrativos.
CAPÍTULO II: Política para dispositivos móviles.	**Artículo:** 6. Protección de los dispositivos móviles con medios de cifrado de datos o mecanismos posteriormente definidas por la Gerencia de Innovación y Desarrollo Tecnológico (GIDT).
CAPÍTULO III: Política de control de acceso lógico.	**Artículos:** 13, 14, 15, 16, 18. Suministro de mecanismos de acceso lógico para la asignación de permisos y responsabilidades de acceso como credenciales y contraseñas.
CAPÍTULO IV: Política sobre el uso de controles criptográficos.	**Artículos:** 20, 21, 22, 23. Apoyo, definición de herramientas, procedimientos y gestión de claves, con responsabilidades activas de información. .

CAPÍTULO V: Política de transferencia e intercambio de información.	**Artículos:** 24, 25, 26, 27, 29, 32. Acciones de mejoramiento, uso de protocolos, y formatos de confidencialidad. Monitoreo de documentos e informaciones almacenadas en impresoras, máquinas y fax.
CAPÍTULO X: Backup copias de seguridad.	**Artículos:** 54, 55, 56, 60, 61, 62, 63. Responsabilidad de la gestión de copias de respaldo de archivos, creación de bitácoras de Backups y comprobación periódica de en los centros de datos.
CAPÍTULO XI: Política de gestión, administración y conservación documental.	**Artículos:** 65, 66, 67, 69, 71, 72, 76. Creación, organización, prevención y control de los archivos, administración de espacios e instalaciones necesarias para la preservación de los mismos.
CAPÍTULO XII: Aplicabilidad.	**Artículos:** 80, 81. Aplicación de todos los procedimientos que conforman el Sistema Integrado de Gestión de la Universidad, en conjunto con medidas disciplinarias administrativas, civil y/o penales.

Por otro lado, la universidad UNAD contiene unas políticas SGSI que, a la fecha están próximas en aprobación para su ejecución, en razón de la protección y conservación de la información del plantel educativo. De esta manera, se muestra una tabla que menciona y puntualiza los puntos que se relacionan con el CSIRT.

Tabla 4. Políticas próximas en aprobación.

CAPÍTULOS	ARTÍCULOS
CAPÍTULO I: Disposiciones generales.	**Artículos:** 1, 2, 3. **Finalidad:** Apoyo en la estandarización de componentes en los campos de acción que afecten la integridad y confidencialidad de la información institucional.
CAPÍTULO II: De los dispositivos móviles.	**Artículo:** 6. **Redes inalámbricas:** Uso de las redes inalámbricas institucionales con fines laborales.
CAPÍTULO III: Del control de acceso lógico.	**Artículos:** 8, 9, 10, 12. **Control:** Acceso lógico para los usuarios, para uso de los recursos, permisos, privilegios y responsabilidades. Creación de credenciales e infracciones en caso de inadecuado uso.
CAPÍTULO IV: Del uso de controles criptográficos.	**Artículos:** 13, 14. **Controles criptográficos:** Implementación de controles necesarios para proteger la integridad y confidencialidad de la información. .
CAPÍTULO XI: De la gestión de incidentes.	**Artículos:** 48, 49, 50. Incidentes: Detección, reporte y evaluación de seguridad de la información que limitan la continuidad de los servicios

De igual manera, es importante la identificación los procesos de gestión de servicios de infraestructura tecnológica, la cual permite identificar las actividades relacionadas al buen funcionamiento de este. De este modo, la tabla presentada a continuación mostrará la información que se relaciona directamente con el CSIRT.

Tabla 5. Procesos PHVA UNAD.

	Procesos
(P) Planear	1. Analizar los requerimientos tecnológicos procedentes de necesidades, servicios, objetivos como institución apuntando hacia las nuevas tendencias tecnológicas. 2. Selección de soluciones tecnológicas a ejecutar. 3. Gestionar los recursos que contemplen el desarrollo y adquisición de actualizaciones de las soluciones tecnológicas. 4. Tener presente las capacidades de los recursos tecnológicos para garantizar disponibilidad y continuidad de los servicios.
(H) Hacer	1. Incorporar la nueva infraestructura tecnológica para soportar los servicios de la institución e implementar soluciones tecnológicas previstas. 2. Gestionar y controlar los accesos a correos, plataformas, aplicaciones y servicios de tecnología. 3. Realización de copias de respaldo de los servidores físicos, virtuales y bases de datos de la universidad UNAD. 4. Coordinar y ejecutar el servicio de mantenimiento de la actual infraestructura.
(V) Verificar	1. Verificar el buen funcionamiento de la infraestructura tecnológica en conjunto de los servicios de solución y mantenimiento de la misma. 2. Monitorear el uso adecuado de los accesos a internet, los servidores y el funcionamiento de todas las plataformas tecnológicas en la misma medida que la operación correcta de soluciones y servicios.
(A) Actuar	1. Gestionar los incidentes de soporte tecnológico. 2. Crear y efectuar cambios y/o restauraciones necesarias durante la operación de los servicios tecnológicos. 3. Tomar decisiones y acciones de mejora para el correcto proceso de monitoreo y desempeño de los servicios tecnológicos.

Es muy importante una vez se tengan definidos los procesos de PHVA identificar los procesos en la atención de incidentes y requerimientos tecnológicos, que nos permitan definir para el CSIRT la gestión de servicios de infraestructura tecnológica en la UNAD;

PROCESO: GESTIÓN DE SERVICIOS DE INFRAESTRUCTURA TECNOLÓGICA

PROCEDIMIENTO: ATENCIÓN DE INCIDENTES Y REQUERIMIENTOS TECNOLÓGICOS:

Objetivo: Brindar atención dentro de los acuerdos de nivel de servicio a los incidentes y requerimientos interpuestos por parte del personal administrativo y docente de la UNAD, que se derivan del acceso, uso y disponibilidad de servicios de Infraestructura Tecnológica-IT necesarios para el desarrollo de sus funciones.

Alcance: Los requisitos establecidos en este procedimiento aplican a todos los servicios IT en producción y comprende desde la administración, seguimiento y solución de incidentes y requerimientos reportados a nivel nacional por el personal administrativo y docente, a través de la aplicación de mesa de ayuda, hasta el análisis y seguimiento a los acuerdos de nivel de servicio establecidos.

Tabla 6. Definiciones, Atención de Incidentes

Concepto	Definición
GIDT	Gerencia de Innovación y Desarrollo Tecnológico
IT	Infraestructura Tecnológica.
Mesa de Ayuda	Aplicación que sirve de único punto de contacto para la recepción de incidentes y requerimientos de IT entre el personal administrativo y docente de la UNAD y la GIDT.
Requerimiento Tecnológico	Necesidad de que se provea hardware, software o insumo tecnológico para el desarrollo de funciones académico / administrativas, y la cual no afecta la operación normal del servicio.
Incidente Tecnológico	Situación imprevista que se presenta en el funcionamiento normal del hardware, software o insumo tecnológico de la UNAD que debe ser solucionado en el menor tiempo posible, por cuanto afecta la operación normal del servicio.
Categoría de ticket	Corresponde al tipo de solicitud registrada en la mesa de ayuda: Incidente o Requerimiento.
Ticket	Solicitud de servicio iniciado por un usuario, en el cual reporta un incidente o requerimiento tecnológico para el buen desarrollo de sus actividades.

Con lo anteriormente expuesto, la importancia de la creación de nuevas normas y regulaciones con unos estatutos ya establecidos, actualizados y modificados, permiten que la propuesta CSIRT sea más acertada en cuanto a la presentación de las

necesidades de seguridad de los datos dentro de un plantel educativo universitario como lo es la UNAD. Por esto, se propone unos lineamientos que contemplen la complejidad que posee la protección y conservación de la información libre, manejable y confidencial.

CAPITULO XIII
POLITICA DE CLASIFICACION DE LA INFORMACIÓN CSIRT-UNAD

Artículo 54. Objetivo del componente de la Clasificación. El contenido de esta política define como el CSIRT-UNAD clasifica la información basados en los distintos niveles de la criticidad.

Artículo 55. Reportes. Las áreas del CSIRT-UNAD, deben apoyar en los procesos de recolección de información de seguridad vital, para así ir implementando estrategias que acompañen la operación interna para determinar medidas de defensa y respuestas.

Artículo 56. Control. El CSIRT-UNAD realizará ejecuciones de pruebas en periodos de tiempos no largos donde se tendrán en cuenta medidas de respuestas basadas en simulacros como si fueran en tiempo real.[53]

CAPITULO XIV
POLITICA DE PROTECCION DE DATOS CSIRT-UNAD

Artículo 57. Objetivo del componente de Protección de datos. El contenido de esta política define, como el CSIRT-UNAD debe proteger la información de acuerdo a su criticidad.

Artículo 58. Norma. El CSIRT-UNAD, contemplando la Norma ISO27001:20058, este aparte del sistema de gestión global la cual se enfoca hacia los riesgos globales para mantener y mejorar la seguridad de la información conservando, la Confidencialidad, integridad y la disponibilidad.[54]

[53] ZAMBRANO HERNANDEZ, Fernando. . Buenas prácticas para establecer un CSIRT nacional Semilleros Ceros y Unos [Sitio web] [Consulta: Agosto de 2021], [Disponible en:]. Obtenido de https://semillerocerosyunos.com/index.php/2021/07/02/buenas-practicas-para-establecer-un-csirt-nacional/

[54] Ibid.; p.81.

CAPITULO XV
POLITICA DE RETENCION DE INFORMACION CSIRT-UNAD

Artículo 59. Objetivo Retención de Información. Definir el tiempo en que se mantendrá retenida la información o los datos recaudados de acuerdo a las políticas del CSIRT-UNAD y de acuerdo a su Ordenación.[55]

CAPITULO XVI
POLITICA DE DESTRUCCION DE INFORMACION CSIRT-UNAD

Artículo 60. Objetivo Destrucción de la Información. Establecer Lineamientos, criterios y actividades para la eliminación de la información o la depuración de los dispositivos que la contengan.

Artículo 61. Norma. Cuando sea estrictamente necesario o cuando está ya se le haya cumplido su ciclo de vida, con el finde que evitar que la información sea restaurada, preservando su confidencialidad e integridad.[56]

CAPITULO XVII
POLITICA DE DIVULGACION DE LA INFORMACION CSIRT-UNAD

Artículo 62. Objetivo Divulgación de la información. Establecer lineamientos acerca de la manera en sé que la información será divulgada.

Artículo 63. Propuesta. Se divulgará con base en dicha necesidad de ser conocida e identificada por parte de agente receptor de los datos.[57]

CAPITULO XVIII
POLITICA DE ACCESO A LA INFORMACION CSIRT-UNAD

Artículo 64. Objetivo Acceso a la Información. Establecer los mecanismos los cuales por medio se podrá obtener acceso a la información.

Artículo 65. Norma. destinar quien deberá acceder a la información con base en la criticidad que se tenga de esta.[58]

---

[55] ZAMBRANO HERNANDEZ, Fernando. . Buenas prácticas para establecer un CSIRT nacional Semilleros Ceros y Unos [Sitio web] [Consulta: Agosto de 2021], [Disponible en:]. Obtenido de https://semillerocerosyunos.com/index.php/2021/07/02/buenas-practicas-para-establecer-un-csirt-nacional/

[56] Ibid.; p.81.

[57] Ibid.; p.81.

[58] Ibid.; p.81.

CAPITULO XIX
POLITICA DE USO APROPIADOS DE LOS SISTEMAS CSIRT-UNAD

Artículo 65. Objetivo Uso Apropiado de los Sistemas. Definir los controles de la seguridad y de esos requerimientos mínimos con los cuales los sistemas de información del CSIRT-UNAD deben contar.

Artículo 66. Propuesta. Controles que peritan restringir el uso estos mismos, únicamente para aquellas labores de la empresa.[59]

CAPITULO XX
POLITICA DEFINICION DE INCIDENTES DE SEGURIDAD Y POLITICAS DE EVENTOS CSIRT-UNAD

Artículo 67. Objetivo de los Incidentes de Seguridad y políticas de Eventos. Esta Política describe los criterios que tiene el CSIRT-UNAD, para determinar la definición de un evento o incidente de seguridad y la clasificación cada uno según el tipo de ataque y la gravedad de la vulnerabilidad.

Artículo 68. Reporte. El NOC “Centro de Operaciones de Red” y El SOC “Centro de Operaciones de Seguridad” serán los encargados del monitoreo continuo de las redes e informarán al CSIRT-UNAD, las definiciones, y las aplicaciones utilizadas en los puntos de acceso final de la red.

Artículo 69. Control. El CSIRT-UNAD definirá los planteamientos y las herramientas para analizar, clasificar e investigar los diferentes incidentes de seguridad ocurridos en la Universidad, esto con el fin de verificar la trazabilidad de los controles implementados.[60]

CAPITULO XXI
POLITICA DE GESTIÓN DE INCIDENTES CSIRT-UNAD

Artículo 70. Objetivo de la Gestión de Incidentes. Lista la implementación del proceso de gestión de incidentes de seguridad de la información.

Artículo 71. Control. Norma para disponer de una capacidad de reacción y respuesta apropiada a los incidentes de seguridad de la información en el CSIRT-UNAD.[61]

---

[59] ZAMBRANO HERNANDEZ, Fernando. . Buenas prácticas para establecer un CSIRT nacional Semilleros Ceros y Unos [Sitio web] [Consulta: Agosto de 2021], [Disponible en:]. Obtenido de https://semillerocerosyunos.com/index.php/2021/07/02/buenas-practicas-para-establecer-un-csirt-nacional/

[60] Ibid.; p.81.

[61] Ibid.; p.81.

CAPITULO XXII
POLITICA DE COOPERACION CSIRT-UNAD

Artículo 72. Objetivo Política de Cooperación. Establece las directrices para la cooperación con las demás entidades, empresas y entes gubernamentales de seguridad informática y CSIRT.

Artículo 73. Propuesta. El CSIRT-UNAD colabora con las investigaciones de incidentes que afecten la seguridad de la información sin interrumpir los tres pilares como lo son; la confidencialidad, la integridad y la disponibilidad. [62]

CAPITULO XXIII
POLITICA DE CUMPLIMIENTO DE LA ETICA Y LA CONFIDENCIALIDAD CSIRT-UNAD

Artículo 74. Objetivo Cumplimiento de la Ética y la Confidencialidad. Establecer las Pautas para la adecuada utilización de los recursos entregados.

Artículo 75. Control. Con base a una cultura de compromiso y honestidad, comprendiendo que la información proporcionada debe tener un manejo de confidencialidad y de ética profesional, así como el de impulsar la educación y la cultura en los equipos de trabajo del CSIRT-UNAD.[63]

CAPITULO XXIV
POLITICA DE CAPACITACION Y ENTRENAMIENTO CSIRT-UNAD

Artículo 75. Objetivo de Capacitación y Entrenamiento. Capacitar y entrenar a todo el personal que conforma el Equipo del CSIRT-UNAD, los ciberataques están en constante evolución.

Artículo 76. Control. Se realizarán evaluaciones y entrenamientos trimestrales de conocimientos y se realizarán pruebas de Test de Penetración y Hacking Ético dentro del equipo CSIRT-UNAD para determinar posibles vulnerabilidades y permanecer en estado de alerta.[64]

---

[62] ZAMBRANO HERNANDEZ, Fernando. . Buenas prácticas para establecer un CSIRT nacional Semilleros Ceros y Unos [Sitio web] [Consulta: Agosto de 2021], [Disponible en:]. Obtenido de https://semillerocerosyunos.com/index.php/2021/07/02/buenas-practicas-para-establecer-un-csirt-nacional/

[63] Ibid.; p.81.

[64] Ibid.; p.81.

8. ORGANIZACIÓN DE ROLES, RESPONSABILIDADES Y FUNCIONES DEL CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS CSIRT-UNAD, POLÍTICAS, PROCESOS Y PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA UNAD.

Desprendida de una estructura adquirida por la adopción e implementación de normas ISO 27000 encargada de la seguridad informática.

Para poder iniciar la definición de los roles y funciones del talento humano del **CSIRT-UNAD** (Equipo de respuestas ante incidentes de seguridad informática de la Universidad Abierta y a Distancia), debemos tener en cuenta aspectos como la organización y administración del equipo de respuesta a los incidentes.

Por tal razón, este equipo será el encargado de mitigar el impacto de las amenazas dentro de la Universidad. Debemos tener en claro que, de acuerdo al crecimiento de las amenazas cibernéticas, éstas se ven elevadas en número y en sofisticación; por lo que es imperativo poseer un recurso humano entrenado, organizado, dirigido y orientado a la realidad en la que estamos inmersos que, si bien estamos sufriendo un escenario de pandemia por el **COVID - 19**, también enfrentamos una pandemia agresiva y desmedida de ciberdelincuencia con ataques de ransomware, malware y demás.

Los **CSIRT**, son entonces el centro de rastreo, preparación y vacuna contra aquellos "virus" que desean llegar en las organizaciones, dicho esto, una de sus funciones o características principal es ser predictivo y proactivo, mas no reactivo después del incidente. En esto se debe tener claro ciertos jugadores que harán parte consistente de todo el ecosistema que se toma en consideración como: la infraestructura, componente principal ya que será la primera en la lista ya que es donde se encuentra alojado el activo vital de operaciones.

Así mismo, la data, ya que estará alojada en servidores de archivos, almacenamiento primario y que puede estar definido en la premisa [65](Datacenter tradicional) o en la nube (soluciones que provienen definidas por software). Por otro lado, la red como factor y

[65] MINISTERIO DE LAS TECNOLOGIAS DE INFORMACIÓN TIC. Guía para la Implementación de Seguridad de la Información en una MIPYME. seguridad de la información, [En Línea] [Consulta: noviembre de 2021], Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

núcleo de operaciones y por donde recorrerá lo valioso de la organización, la información, y es el punto neural que posee toda la atención, donde la creación de capa de aplicaciones debe estar definirlas como misionales y operativas. Continuado de, el usuario final quien será el foco de atención principal ya que será a quien se le realice el ataque o por donde puede ingresar uno.

No obstante, Se debe tener en cuenta, antes de iniciar una implementación y puesta en marcha de un CSIRT, se tiene que generar y madurar una cultura seguridad de la información dentro de la organización para así difundir, afianzar y aplicar las políticas de cuidado y preservación de la información.

Así mismo hay que tener presente ciertas características para su organización y administración y las responsabilidades claves del **CSIRT-UNAD**, así:

1. Investigar y analizar incidentes.
2. Crear y mantener un plan de respuestas a incidentes.
3. Gestionar las comunicaciones internas y las actualizaciones.
4. Comunicarse con la comunidad Unadista en general, como son: los estudiantes, profesores, directores y administrativos para obtener información de incidentes según sea necesario.
5. Recomendar cambios en la tecnología, las políticas aplicadas, el sistema de gobierno y la capacitación después de un ataque, a esto lo definiremos como la lección aprendida.

Es importante determinar la diferencia entre un **CSIRT** y un **SOC**, esto debido a la existencia de responsabilidades superpuestas entre el uno y el otro, para ello lo aclararemos así: el **Centro de Operaciones de Seguridad (SOC)**, es una instalación donde se monitorea y se defiende la red, las aplicaciones (misionales, operáticas y uso no frecuente) y los puntos de acceso final de la red, que serían para nosotros el estudiante, profesor o empleado de la comunidad Unadista. Este **SOC**, se desprende del **Centro de Operaciones de Red (NOC)** quien es el verdadero encargado del monitoreo continuo de las redes con que cuenta una organización.

El origen del término **"Equipo de respuesta ante emergencias informáticas"** toma lugar en 1988 ante el ataque del gusano Morris[66] que afectó a los servidores del programa

[66] PERIODISTA DIGITAL. El Gusano Morris y los daños que causó en Internet [Sitio web], [Consulta: 16 de julio de 2019]. Disponible en:https://www.periodistadigital.com/tecnologia/tec-internet/20190726/gusano-morris-danos-causo-internet-noticia-689404036001/

DARPA[67] que nace cinco años después de la aparición comercial de internet perteneciente a la Agencia de Proyectos de Investigación Avanzada de Defensa y apoyaba a la red de redes, su creación va enfocada con el fin de recopilar y difundir información sobre vulnerabilidades críticas sobre la red y que responderá con su propia infraestructura, a esto se conoce como **CERT**. Por lo anterior el **CSIRT-UNAD** será el encargado de dar respuestas integrales incluyendo tanto las acciones técnicas tomadas para la remediación del incidente como los cambios y las recomendaciones para la protección en el futuro, de igual manera, los aspectos a considerar serán las acciones no técnicas que el **CSIRT-UNAD** debe adoptar como las acciones y el tratamiento legal sobre cualquier problema de personal en caso de acciones internas que hayan generado el riesgo informático, dada esta razón el **CSIRT-UNAD** es un equipo multifuncional.

Figura 5. Explicación de la relación del CSIRT-UNAD y un SOC Prevención, respuesta y políticas de prevención.

Fuente 6 Elaboración Propia

[67] DEFENSE ADVANCED RESEARCH PROJECTS AGENCY. Creando innovadoras tecnologias y capacidades por la seguridad nacional [www.darpa.mil]; [Consulta: 20 de Julio de 2021]. Disponible en:https://www.darpa.mil/

Para todos los roles que a continuación se describen, es preciso que cada miembro deba tener una persona de backup o figura de suplente o esquema de respaldo del principal, también debemos considerar que debe existir un equipo de monitoreo que actúe en 7/24 en esquemas de trabajo de 3 turnos de 8 horas como mínimo y así evitar la fatiga de quienes realizan las tareas de cuidado y protección. Esto se debe prever debido a que los ciberdelincuentes y sus amenazas nunca descansan y siempre están buscando la mejor oportunidad para dirigir un ataque.

¿a futuro como será estructurado? conformando un equipo de talento humano y se delimitarán los roles y funciones que estarán inmersas dentro del **CSIRT-UNAD** y quienes de ahora en adelante cumplirán sus funciones de seguridad dentro de la seguridad. Con ello, las funciones serán predictivas y reactivas y tendremos como figura referencial que el **CSIRT-UNAD** será el de ahora en adelante actuará como el centro de crisis y toma de decisiones ante un ciberataque[68].

Para esto es necesario que el **CSIRT-UNAD** adopte ciertas políticas existentes en la universidad y que han sido implementadas en el sistema de gestión y seguridad de la información, como también adquirirá estas mismas con un proceso de afinamiento si hay lugar a ello, en el mismo orden de ideas el CSIRT-UNAD, pretende estar presente y en forma activa en la evaluación y proposición de nuevas políticas de seguridad de la información, debido a que será el uno de los responsables directos de la evaluación, detección y mitigación de cualquier evento real, sospecho o falso positivo que pueda afectar el buen funcionamiento de los sistemas lógicos y físicos con que cuenta la universidad; será de igual manera un actor activo sobre la evaluación de las políticas y el futuro impacto que las posibles vulnerabilidades lleguen a ejercer al interior de la universidad, siempre teniendo en cuenta la valoración del daño del ambiente como también el daño que puede haber en la reputación de la institución educativa.

En cuanto al impacto o la actuación del **CSIRT-UNAD**, este tendrá un campo de operaciones dentro de toda la comunidad Unadista, debido a que la ciberdelincuencia no aísla a un solo sector de una organización, pero su centro de atención siempre será el salvaguardar y proteger la infraestructura critica de la entidad **(Data Center).**

[68] SECURESOFT , Corporation. ¿Cómo organizar un CSIRT?Un equipo de respuesta a incidentes de seguridad informática (CSIRT) puede ayudar a mitigar el impacto de las amenazas a la seguridad de cualquier organización[Sitio web],[consulta: 20 de julio de 2018] Disponible en: https://securitysummitperu.com/articulos/como-organizar-un-csirt/

Las habilidades y experiencia que debemos tener en cuenta para el **CSIRT-UNAD**, es contar con un grupo no solo dedicado al monitoreo continuo de la infraestructura física, lógica y en general del ecosistema de operaciones de la universidad, que se vean involucrados en actividades de continua investigación acerca de las nuevas modalidades emergentes de ciberdelincuencia. El **CSIRT-UNAD,** se complementará ejecutando una tarea de comunicación con **CSIRT** externos que tengan relación con el sector de la educación y apoyado en un proceso de recolección de información vital de seguridad para así ir implementando estrategias que acompañen la operación interna y poseer medidas de defensa y respuesta.

Otro punto clave de experiencia que se debe tener en cuenta, es realizar ejecuciones de pruebas en periodos de tiempo no largos es decir con periodicidad no inferior a 4 meses donde se tendrán en cuenta las medidas de respuesta basados en simulacros como si fuera en tiempo real.

Esta actividad de simulacros recreados debe ser específicos y crecientes, es decir escoger una aplicación o servicio puntual donde se mida la forma de realizar el ataque, como un ataque de fuerza bruta, donde se puede promover un ataque aleatorio de inicio de sesión con un usuario y contraseña aleatoria perteneciente a algún miembro de la universidad tanto en calidad de estudiante como trabajador, realizar una detección y prevención de intrusiones a través de logs o panel de control del firewall de siguiente generación (NGFW)[69] o consola de administración del EDR (plataforma de protección de punto final) que es la evolución de los NGAV (antivirus de siguiente generación), realizando la implantación de un malware y por ultimo valorar y generar un informe de control de daños instantáneos donde se verá reflejado la exposición a la vulnerabilidad. Este mismo ejercicio se deberá aplicar a servidores y almacenamiento al punto de llegar a medir la afectación total del Data Center.

Finalmente este ejercicio llevara a tener una capacitación continua en paralelo al desarrollo de las actividades del día a día que conllevaran al fortalecimiento de las mejores prácticas de atención ante un incidente de seguridad cibernética, esto permitirá tener un desarrollo acertado de respuestas a incidentes, de igual manera así se reconocerán las ciber amenazas más comunes y se comprenderán a los actores de las amenazas, los componentes de una cadena de muerte cibernética (compromiso total de

[69] FORTINET. www.fortinet.com,Next-Generation Firewall (NGFW)[Sitio Web]el filtrado de paquetes, la compatibilidad con IPsec y VPN SSL[Consulta 2021] Disponible en: https://www.fortinet.com/lat/products/next-generation-firewall

la data encriptándola o borrándola y la afectación de los servidores ya sean físicos o virtualizados acabando con sus componentes).

Estas tareas se realizan con el fin de cuidar la infraestructura critica de la **UNAD** y es por eso que el **CSIRT-UNAD** esta presto a la defensa de la infraestructura que es considerada estratégica por estar relacionada con la provisión de servicios esenciales y que cuya afectación pudiera comprometer el correcto funcionamiento de la universidad.

En este punto se abarcan las definiciones, características y funciones de un **CSIRT**, por ello se debe entrar a definir la estructura de liderazgo y responsabilidad dentro del **CSIRT**, como se es mencionado es un equipo multifuncional que se coordinara durante la presencia de un incidente.

Por política de creación es imperativo que el **CSIRT-UNAD** deba tener reuniones trimestrales conjuntas para el afinamiento, divulgación y aplicación de las políticas de seguridad, como la entrega de las estadísticas de brechas y riesgos informáticos, así mismo se debe analizar nuevas herramientas de cuidado como entrenamiento y prevención, como antídoto al equipo técnico como refuerzo a su conocimiento (Educación interna continua), por lo anterior, deberán generarse en la primera semana del mes de inicio de cuarto de año; en estas reuniones se debe gestionar un plan de simulacros de al menos tres por año donde se tendrá por consideraciones los incidentes en la mesa, es aquí donde se evaluara como se actúa, que se haría en caso de un incidente real y el equipo de mantenga alerta y dispuesto a resolver cualquier incidente de la manera idónea y técnica, sin la afectación de la funcionabilidad de la Universidad, cabe anotar que estas políticas y mediciones serán tenidas en cuenta tanto para valoración de riesgo externo como interno general y especifico, esto debido a que la Universidad cuenta con una facultad de ingeniería de sistemas y un programa de especialización en seguridad informática donde se imparten cátedras que van relacionas con al impacto de los vulneraciones y por prácticas de los estudiantes la infraestructura se puede ver comprometida.[70]

[70] SECURESOFT , Corporation. ¿Cómo organizar un CSIRT?Un equipo de respuesta a incidentes de seguridad informática (CSIRT) puede ayudar a mitigar el impacto de las amenazas a la seguridad de cualquier organización[Sitio web],[consulta: 20 de julio de 2018] Disponible en: https://securitysummitperu.com/articulos/como-organizar-un-csirt/

Líder de equipo CISO: es un personal de nivel directivo y será de ahora en adelante el puente ente en la alta dirección (rectoría) y el comité general de calidad.

CISO

Rol: será el encargado de proveer la información del estado de evaluación de los riesgos, la afectación de servicios y comunicar de forma ejecutiva los incidentes dentro de la organización.

Función: será responsabilidad del **CISO**, asegurar la atención y el presupuesto para que el **CSIRT-UNAD**, funcione de manera idónea, recomendara de igual manera ante la parte administrativa la adquisición de nuevas herramientas como activos lógicos o físicos, para brindar una mejor seguridad, una vez estás sean evaluadas previamente por el **CSIRT-UNAD** y el fabricante o quien haga sus veces de representante en el país.

Perfil: Deberá tener un título profesional en ingeniería de sistemas o afines con una especialización y/o maestría en seguridad de la información e indicará a su equipo las estrategias de trabajo, evaluación y capacitación continua, como también la aplicabilidad de la lección aprendida deriva de ataques anteriores.

Administrador de Incidentes: Será un profesional de nivel administrativo.

ADMINISTRADOR DE INCIDENTES

Rol: responsable del conocimiento del comportamiento de toda la infraestructura recibiendo la respectiva información de los administradores ajenos al equipo, como es el administrador de red, administrador de aplicaciones, administrador de infraestructura, administrador de servicios en la nube y administrador de recursos físicos de los usuarios finales (pc, portátiles, impresoras, cctv, control de acceso), administrador de los ambientes de desarrollo y pruebas, decano de la facultad de ingeniería.

Función: será el responsable de convocar las reuniones y de delegar las responsabilidades a los miembros del equipo de acuerdo a la asignación de los elementos de acción, será el encargado de valorar la matriz de riesgos en los activos físicos y lógicos con los que cuenta la Universidad para su asignación e informara al CISO del desempeño general del equipo.

Perfil: ingeniero de sistemas o afines con conocimiento o certificaciones en sistemas de protección de datos, seguridad informática, ethical hacking y metodología ITIL

Investigador Principal: Este es un recurso técnico.

INVESTIGADOR PRINCIPAL

Rol: será el analista en jefe y velara por el análisis de los incidentes y procederá como respondiente de incidentes dentro del SOC, deberá investigar los sucesos que dieron lugar al incidente determinando la causa inicial y final.

Función: Coordinar y llevar a cabo la investigación de las posibles vulnerabilidades, incidentes y/o amenazas, esta tarea estará apoya por las diferentes herramientas de informática forense con que cuente la Universidad y de igual manera involucrara un recurso humano de mínimo dos investigadores de incidentes que estarán apoyando su labor, generando ambientes tipo Sandboxing, que son ambientes controlados para determinar las características de las amenazas, su comportamiento y el impacto dentro de la organización, cabe aclarar que este ambiente no es lo mismo que el ambiente de pruebas con que cuenta el área de desarrollo o las áreas que requieren un espacio de prueba de aplicaciones o servicios.

Perfil: puede ser tecnólogo en sistemas o ingeniero de sistemas con certificaciones o énfasis de estudio en sistemas de seguridad informática y conocimientos de informática forense.

Investigador Auxiliar: Este es un recurso técnico.

INVESTIGADORES AUXILIARES

Rol: seran analistas de primer y nivel velara por el monitoreo y análisis de los incidentes y procederán a ser los primeros respondientes ante una alerta de incidente que se manifieste dentro del SOC, deberán investigar los sucesos que dieron lugar al incidente determinando la causa inicial y final y estaran coordinados por el investigador principal.

Función: Llevaran a cabo la investigación de las posibles vulnerabilidades, incidentes y/o amenazas, deben estar distribuidos por control de herramientas asignadas para este fin, contando con utilidades de informática forensede acuerdo a la instrucción del investigador principal recrearan y generaran los ambientes de prueba tipo Sandboxing, que son ambientes controlados para determinar las características de las amenazas, su comportamiento y el impacto

Perfil: puede ser tecnólogo en sistemas o ingeniero de sistemas con certificaciones o énfasis de estudio en sistemas de seguridad informática y conocimientos de informática forense.

Comunicador Social o Cummunity Manager: Recurso de nivel Profesional o tecnólogo.

Rol: Responsable del manejo de la información y publicación informativa sobre la seguridad y los incidentes, estará en continua comunicación con el **CISO**, quien será el encargado de aprobar los contenidos como también la clasificación de las comunicaciones, como información reservado dentro del CSIRT-UNAD e información publica..

Función: Será el encargado de administrar la información que se compartirá a nivel interno de la Universidad como comunicados a nivel externo en las plataformas informativas con las que cuenta la Universidad, de igual manera será el responsable de diseñar y poner en marcha al menos dos campañas mensuales generando una cultura de ciberseguridad promoviendo las políticas que la Universidad adopto.

Perfil: Podrá ser tecnólogo en comunicación social o profesional en comunicación social y periodismo, deberá tener conocimiento en administración de redes sociales y análisis del impacto de la información, manejo de medios y generación de boletines.

Abogado: Recurso profesional en derecho.

Rol: Permanecerá en contacto con el **CISO**, quien le dará las directrices de actuación frente a alguna acción legal que requiera el manejo, será de igual manera el puente de comunicación entre las autoridades competentes en caso de requerir su intervención como Policía Nacional, Fiscalía o algún ente del orden nacional o distrital que requería conocimiento y manejo jurídico. Trabajara de la mano también con recursos humanos en caso de requerir la aplicación de correctivos legales al interior de la institución.

Función: Será el encargado de velar por el cumplimiento de la legislación existente en el territorio nacional acerca de ciberseguridad y delitos informáticos como también la jurisprudencia que se aplica al tratamiento de datos personales.

Perfil: Deberá ser profesional en derecho, preferiblemente con especialización en derecho de las tecnologías de la información.

Talento Humano: Recurso profesional en Psicología organizacional o profesional con carreras afines con especialización en gestión del talento humano.

TALENTO HUMANO

Rol: Permanecerá en contacto con el **CISO**, con el comunity manager y el abogado, quienes serán los encargados de brindarle información de lo que esta sucediendo al interior de la institución, de igual manera esta sujeto a apoyar las campañas de promoción de la cultura de la seguridad informática dentro de la Universidad con el fin de reforzar su aplicabilidad, el represéntate de talento humano apoyado con el área legal será el encargado de acuerdo al reglamento interno de aplicar los correctivos que halla necesidad en caso de alguna violación de las políticas de seguridad.

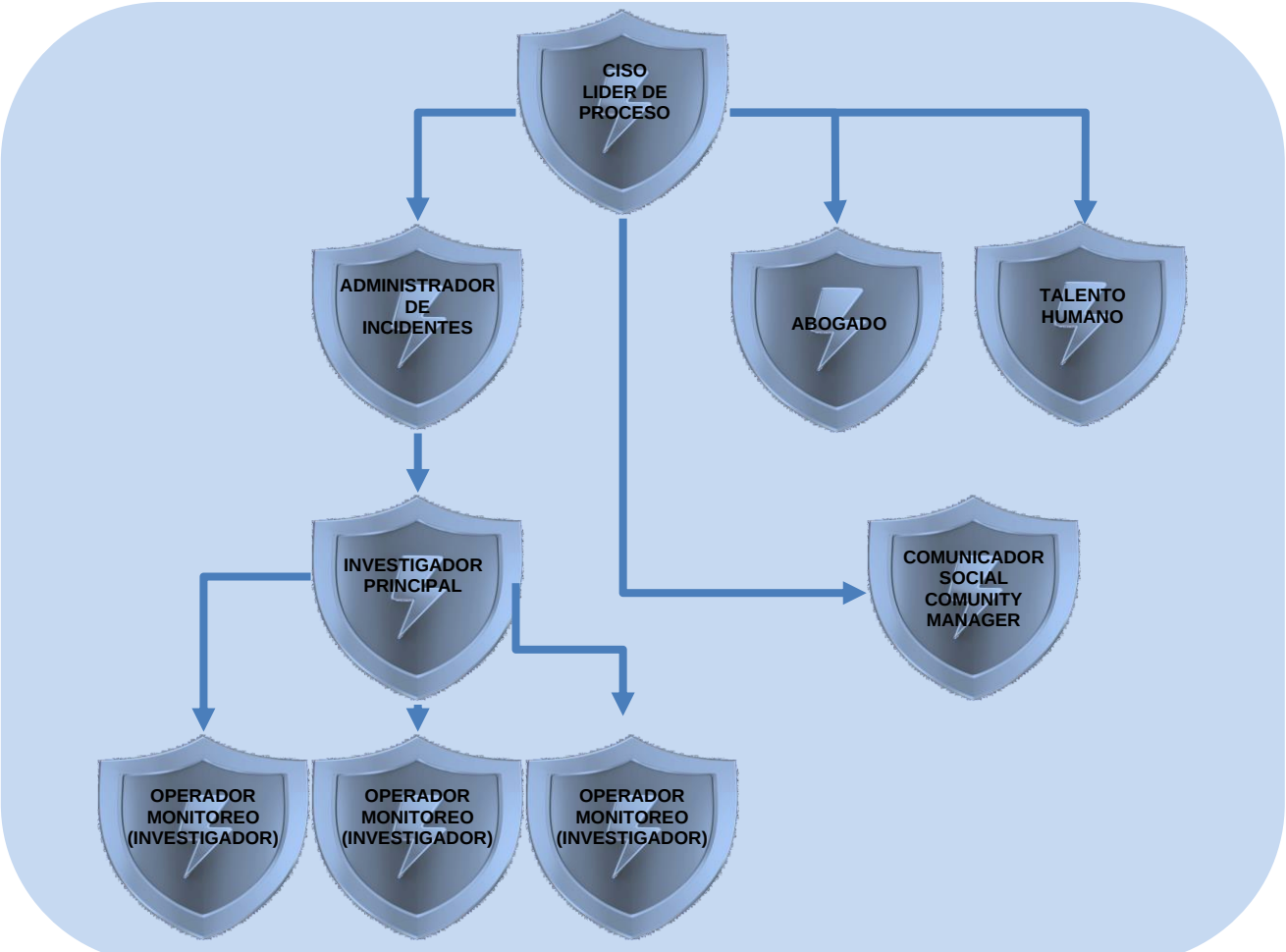
Función: Será el encargado del manejo de situaciones donde se vean involucrados miembros o colaboradores que laboran con la Universidad en calidad de contratistas, empleados directos, docentes de planta, docentes hora catedra y otros, cuando se vea vulnerada información privilegiada o sensible y que se haya desprendido la acción de un incidente o vulnerabilidad.

Perfil: Deberá ser profesional en Psicología organizacional o carreras afines con especialización en gestión del talento humano, preferiblemente será el líder del proceso de Talento Humano de la Universidad o un delegado con este mismo con poder de toma de decisiones.

Una vez estructurado y socializado al interior del equipo, el líder de este **CSIRT-UNAD** tendrá la responsabilidad de socializarlo a la rectoría en comité para su aprobación mediante resolución de conformación y es aquí donde se asegura y confirman los roles y responsabilidades del CSIRT-UNAD y es así como se establecerá su estatuto de operaciones, esto quiere decir que se socializará su manera de operar y el establecimiento de un protocolo de actuaciones como por ejemplo: en caso de inicio de un ataque, quien será el encargado de elevar la alarma y la primera llamada, actividades de contención, con que periodicidad de tiempo se estará informando el estado de la situación y la elaboración de aprobaciones para dar continuidad o bajar los servicios comprometidos y su forma de actuación para la restauración[71].

[71] COLCERT. Grupo de Respuesta a Emergencia Cibernetícas de Colombia[www.colcert.gov.co] [Sitio web]organismo coordinador a nivel nacional en aspectos de ciberseguridad y ciberdefensa del Estado[Consulta: Enero 2021]Disponible en:https://www.colcert.gov.co/

Figura 6. Gráfica de jerarquización del CSIRT -UNAD



Fuente 7 Elaboración Propia

Ahora bien, una vez definido el **CSIRT-UNAD** en su estructura y en su aprobación y de igual manera haber sido aprobado su funcionamiento este debe tener la capacidad de solicitar al área de talento humano de la universidad un procedimiento de contratación especial del personal, debido a que debe existir un estudio de control y confianza, esto derivado a que el equipo será el encargado de la seguridad de la seguridad de la información de toda la comunidad Unadista, por lo que sugiero tener en cuenta estas propuestas para el proceso así:

Figura 7 de esquema CONTROL Y CONFIANZA

Fuente 8 Elaboración Propia

Esto con el fin de evitar casos como el de Edward Snowden, quien fue el que revelo el espionaje masivo de estados Unidos e incurrió en la extracción de información dentro de la organización donde trabajaba y el caso de Frances Haugen quien sustrajo y publico archivos de integridad cívica de Facebook.

1. Recepción, análisis y verificación de la información y documentación suministrada por el o los aspirantes al equipo CSIRT-UNAD.
2. Identificar las características de personalidad enfocadas en su inteligencia y habilidades del o los aspirantes al equipo CSIRT-UNAD.
3. Evaluación para detectar rasgos de actuación y medir el nivel de confianza con el manejo de la seguridad de la información, aplicable tanto a los aspirantes como al equipo en producción del CSIRT-UNAD.

4. Prueba que se realiza como examen de ingreso y periódico para dar cumplimiento al SGSST y detectar el estado médico del aspirante como del equipo de producción del CSIRT-UNAD.
5. Rastrear y controlar el no consumo de sustancias psicoactivas para evitar el mal comportamiento que derive en una mala práctica de las tareas asignadas, se debe aplicar tanto al aspirante como al equipo de producción del CSIRT-UNAD.

Figura 8 de esquema CATALOGO DE SERVICIOS CSIRT-UNAD

Fuente 9 Elaboración Propia

9. FORMULAR PLAN MAESTRO ESTRATÉGICO ENFOCADO A LA ATENCIÓN DE EVENTOS CIBERNÉTICOS Y AFIANZADO EN LA CULTURA DE CIBERSEGURIDAD.

En coordinación con el área de TI en especial con el área de SGSI se deben incluir las políticas y procedimientos de acción y prevención enfocados a la continuidad de las operaciones.

Por lo tanto se justifica la implementación de un **CSIRT-UNAD**, motivado a la preservación e integridad de los datos de toda la comunidad Unadista y que de igual manera cuidara de la inversión en plataformas tecnológicas ya que sin una precaución segura y aplicada a las **normas ISO**,[72] haría una perfecta oportunidad para que cualquier personaje inescrupuloso se apoderarse del bien más preciado, la información, (**LA DATA**), donde se puede ver reflejado el bajar el costo de inversión con un retorno de esta misma, la mejor infraestructura nunca podrá ser buena sin una excelente seguridad, que se encuentre estructurada, definida, difundida y aplicada.

La oficina de **TIC** deberá ser la responsable del monitoreo continuo de su infraestructura a nivel de que reporte a diario la condición de la o las redes que posea; como también del estado físico y lógico de los sistemas. Será también la directa responsable de la actualización de los sistemas operativos (parches), como también de los microcódigos (firmware), no sin antes validarlos con los respectivos fabricantes y la veracidad de las firmas de estos y así mitigar los posibles riesgos de pérdida o corrupción de la información, ya sea en un dispositivo físico y/o lógico (servidores, almacenamiento y switches).

Al **CSIRT-UNAD**, se le deberán asignar tareas de seguridad y control tanto del área de sistemas como de todos los procesos transversales en donde la oficina de **TIC** se vea involucrada o tome presencia, será de ahora en adelante el punto de control de la información de los incidentes cibernéticos para tener un control medible cualitativo como cuantitativo del riesgo y jugara el papel de coordinador primario de la toma de decisiones frente a un posible ataque en ejecución.

[72] ISOTOOLS. La familia de normas ISO 27000.[www.isotools.org][Sitio web]Esta estandarización contiene las definiciones y los términos que se utilizarán durante toda la serie 27000.[Consulta: 21 de Enero de 2015] Disponible en:https://www.isotools.org/2015/01/21/familia-normas-iso-27000/

Figura 9 Análisis de Riesgos

Fuente 10 Elaboración Propia

De esta forma, también deberá brindar un control interno de información, como la valoración externa de la infraestructura completa y colaborar con entes externos para la mitigación del riesgo que cumplan sus mismas funciones, como el **CSIRT** de la Policía Nacional de Colombia.[73]

Por otro lado, el **CSIRT-UNAD** interno, debe recolectar toda la información de las diferentes facultades, áreas de funcionalidad y operativas donde se vea involucrado el manejo de información digital o que ha sido digitalizada en la alimentación de procesos dentro de la institución, por lo cual, deberemos valorar una matriz de peligros para delimitar un mapa de riesgo e importancia del acceso a la información.

Es entonces que, con lo anterior, se deben definir etapas de acción y gobierno dentro de la oficina de TIC; así:

- **Primera etapa (predictiva):** Estará cubierta por acciones como: administración de alertas y advertencias derivadas de las herramientas de control de seguridad (antivirus, firewall, entre otros); generar y controlar el apoyo para el manejo de

[73] COLCERT. Grupo de Respuesta a Emergencia Cibernetícas de Colombia[www.colcert.gov.co] [Sitio web]organismo coordinador a nivel nacional en aspectos de ciberseguridad y ciberdefensa del Estado[Consulta: Enero 2021]Disponible en:https://www.colcert.gov.co/

incidentes identificando las vulnerabilidades para crear las respuestas y acciones prioritarias de mitigación y así levantar un tablero de control de estadísticas.

- **Segunda etapa (proactiva):** Desarrollar, investigar y adoptar herramientas valoradas y testeadas a nivel regional e internacional para brindar la efectiva detección de presuntos ataques o intrusos dentro de la red Unadista y de igual manera la divulgación oportuna y temprana de la información de las amenazas públicas para así tener una perspectiva tecnológica real y avanzada.

- **Tercera etapa (calidad de la seguridad):** Donde se deberá tener la coordinación de una estrategia de recuperación ante un ciber desastre dentro de la infraestructura tecnológica con la que cuenta la **UNAD, (DATACENTER FISICO-VIRTUAL),** manteniendo una continua política de educación, concientización y divulgación de las políticas de seguridad. Por último, la evaluación y puntuación de las aplicaciones o herramientas con las que cuenta y contará la **UNAD** a nivel tecnológico.

La implementación del **plan estratégico CSIRT-UNAD**,[74] nos permitirá saber las medidas efectivas de ciberseguridad, esto es particularmente desafiante hoy porque hay más dispositivos que personas y los atacantes se están volviendo más innovadores. El objetivo será ayudar a comprender las funciones básicas de un marco de seguridad y la importancia de establecer ciberseguridad para proteger la información basada en los tres pilares de la seguridad de los datos.

Iniciado este recorrido de la implementación y afinamiento del **CSIRT-UNAD**, debemos tomar como primera acción una vez jerarquizado y delegado las funciones del equipo la creación y adopción de un plan de respuestas a incidentes donde se verán inmersas las políticas existentes como también su modificación, inserción y afinamientos de las que al momento estén en análisis para su implementación.

Para esto deberemos contar con la ayuda y el apoyo de la facultad de ingeniería de sistemas y en especial de su programa especialización en seguridad informática, ya que son los **expertos consultores** que ayudarán a crear el plan maestro de respuestas a incidentes y qué políticas son las más apropiadas para la implementación, de acuerdo al

[74] MINISTERIO DE EDUCACIÓN NACIONAL. Plan estratégico de de tecnologias de la información 2019/2022[En linea]gestionar los recursos de tecnología de la información[Consulta: Enero de 2019] Disponible en: https://www.mineducacion.gov.co/1759/articles-362792_galeria_11.pdf

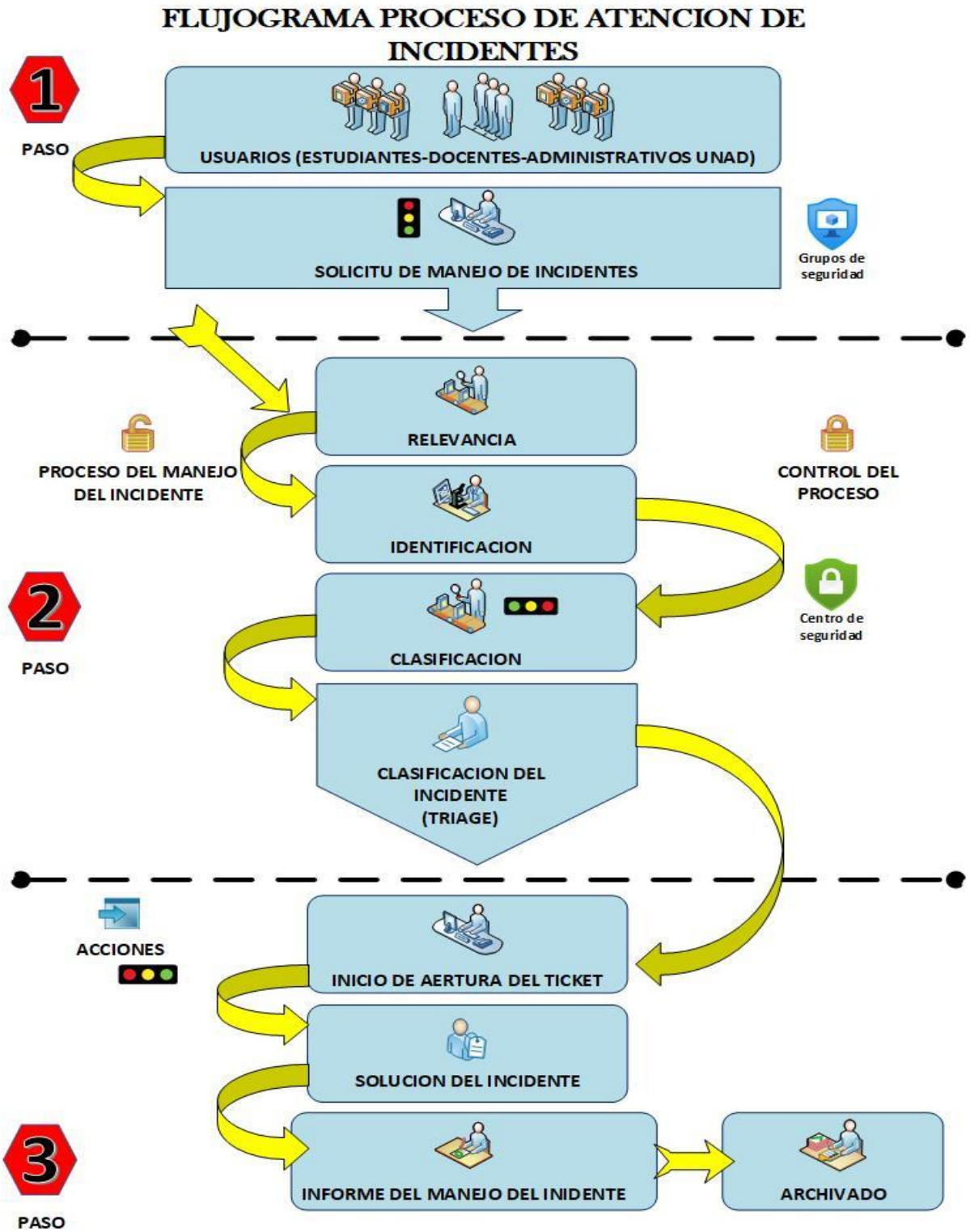
sector de educación, estos actuaran en calidad de **consultores externos**, para que coadyuven en las operaciones del **CSIRT-UNAD,** siendo así como colaboran en la elaboración de los procesos de implementación de acuerdo a las normas técnicas nacionales e internacionales que influyen en el buen funcionamiento de este.[75]

Es importante que todo el grupo este familiarizado con la infraestructura con que cuenta la universidad y en especial posean un alto nivel de sentido de propiedad ya que esto hará que se articule de mejor manera las políticas en general.

Se debe apreciar y adoptar recursos para la publicación de este plan de respuesta a incidentes, apoyados en material visual y de fácil consulta, ya que, en caso de respuesta inmediata a presión, sea fácil de encontrar cómo consultar; estos pueden ser: infografías, cartillas rápidas digitales, presentación en PowerPoint, documento en hoja de cálculo o documento en PDF.

[75] MINISTERIO DE EDUCACIÓN NACIONAL. Plan estratégico de de tecnologias de la información 2019/2022[En linea]gestionar los recursos de tecnología de la información[Consulta: Enero de 2019] Disponible en: https://www.mineducacion.gov.co/1759/articles-362792_galeria_11.pdf

Figura 10 Flujograma de Procesos de atención de Incidentes.



Fuente 11 Elaboración Propia

Una vez se genere el plan de respuestas a incidentes este debe ser sometido a socialización al interior del equipo para su análisis y observaciones, como también para su aprobación del director y equipo de Tecnología de Universidad, este a su vez lo socialice y lo exponga ante la rectoría en comité para proceso y avance de la resolución. Para certificar lo anterior, se debe tener una documentación actualizada de los activos críticos, aquí la claridad en la catalogación de estos activos es importante, ya que, estarán inmersos los sistemas críticos, como los de propiedad intelectual o de desarrollo inhouse, esto con el fin de comprender realmente el valor del código fuente creado de propiedad de la **UNAD.**

De este modo, esta documentación debe tener un valorado de acuerdo al impacto económico y de reputación en caso de llegar a tener una caída parcial o total de servicios por causa de un incidente. En este caso, es necesario valorar las bases de datos de acuerdo a su criticidad funcional y sectorizarlas por misionales y críticas, además de ser catalogadas como de almacenamiento académico (documentos de consulta) o almacenamiento académico de recolección de información de personal (datos de estudiantes, docentes, directivos y colaboradores en general). Y, por último, las bases de datos administrativas criticas (CRM o software contable y de manejo de nómina).
En este mismo orden, se permite tener esta documentación de forma coherente y organizada, los conceptos, hallazgos y acciones de mejora obtenidas como resultado de las auditorias previas realizadas a los sistemas de gestión de la información que han sido ejecutadas previo a la conformación del **CSIRT-UNAD,** esto conducente a tener claro los tiempos de atención en caso en un incidente como se explica a continuación.

Figura 11 Línea del tiempo de atención.

Fuente 12 Elaboración Propia

Por lo anterior y antes expuesto se debe tener en claro la definición para la universidad de lo que es la infraestructura crítica, debido a que, esta está considerada como estratégica por ser quien provisiona los bienes y servicios esenciales y que cuya afectación puede comprometer la continuidad de operaciones de la universidad.

Cuando se habla de transformación digital y seguridad de la información, como también del concepto de continuidad de negocios, se debe valorar que todo el hardware instalado tiene por regla un esquema de clúster o de alta disponibilidad (HA), como también un esquema de Datacenter alterno ya sea onpremise en un sitio totalmente diferente a las instalaciones de la universidad o en algún proveedor de servicios en la nube. Cabe anotar que si se referencia a nube (cloud) esta únicamente deberá ser para los sistemas críticos de operación.

En continuidad a lo anterior, se consideran las acciones de revisar y probar el plan de recuperación de desastres y las políticas de **backup**, debido a que, en un alto porcentaje se dependerá de este para el restablecimiento de los servicios de la universidad, para eso el área encargada debe proveer los tiempos exactos **de RPO y RTO** y asimismo el manejo del esquema de alta disponibilidad y la presentación del plan de recuperación de desastres. Con esto el **CSIRT-UNAD** se apoyará en caso de que la afectación logre corromper, encriptar, secuestrar o borrar la información, como también las aplicaciones.

Todo lo anterior, se lo debe tener claro, ya que el punto central y neural será el Datacenter que es donde se alojan servidores, redes, almacenamiento y otros equipos de TI que permiten el funcionamiento de la universidad, los servidores de un centro de datos contienen o facilitan aplicaciones, servicios y datos esenciales para la universidad y sus estudiantes.

Las instalaciones del Datacenter deben conservar las siguientes características: disponibilidad, escalabilidad, seguridad, manejabilidad y desempeño; esto con el fin de cumpla con la normatividad de Tiers.

De tal modo que sea consecuente en la ejecución de las tareas, por esto la realización de una valoración de riesgos es importante en los procesos que debe estar enfocada tanto en el software como en el hardware con que cuenta la universidad y que se puede tomar como marco de referencia la norma ISO 31000[76] que habla de la administración o gerenciamiento del riesgo así:

[76] ISO 31000,GESTIÓN DE RIESGOS;[Sitio web].evaluar y actualizar continuamente su oferta hasta optimizar sus procesos.[Consulta: octubre 19 2021]Disponible en:https://www.iso.org/iso-31000-risk-management.html

Figura 12 Análisis de Riesgos.

Fuente 13 Elaboración Propia

Ya habiendo ejecutado la matriz de valoración de riesgos[77] se debe tener en cuenta la protección de los activos, siempre pensando que estos se refieren tanto al hardware como al software que la **UNAD** posee, para esto tendremos en cuenta los siguientes aspectos:

1. Gestión de la Seguridad.
2. Gestión de Crisis.
3. Seguridad de la Información.
4. Aplicaciones.
5. Investigación.
6. Operaciones del Oficial de Seguridad.
7. Seguridad Física.

[77] ISO 31000,GESTIÓN DE RIESGOS;[Sitio web].evaluar y actualizar continuamente su oferta hasta optimizar sus procesos.[Consulta: octubre 19 2021]Disponible en:https://www.iso.org/iso-31000-risk-management.html

Todo esto se describe y se involucra dentro del **CSIRT-UNAD, ya como parte activa de su plan estratégico de actuación,** este será el encargado de manejar información muy sensible, es una buena práctica que, así como toma control de monitoreo de toda la parte de infraestructura lógica y física del centro de datos perteneciente a TI, este sea el encargado también en compañía de la o las empresas de seguridad de tomar el control físico de las instalaciones de la Universidad.

Para este fin el **CSIRT-UNAD**, en su **plan de acción** gestiona lo siguiente:

- **Reglas generales para el control y monitoreo de la sede.**

    1. Usar controles de acceso ya sean por medio de lectura del carnet de trabajador o estudiante y/o reconocimiento facial tanto al ingreso y egreso de las instalaciones como para áreas restringidas o sensibles.

    2. Hacer que la oficina del **CSIRT-UNAD,** solo tengan acceso los integrantes del equipo y de igual forma no identificarla con el nombre del sitio, sino por el contrario usar nombres de ciudades mundiales para que la oficina no quede expuesta en su ubicación, así mismo se deberá de nombrar el centro de datos y las áreas que se vean involucradas con la gestión de TI.

    3. Implementar un sistema de CCTV para poder monitorear los alrededores de las instalaciones de la universidad como también las oficinas, zonas de ingreso y áreas comunes.

    4. Se debe restringir el uso de celulares o dispositivos móviles en las áreas de presencia de información sensible.

- **Reglas generales para los equipos de TI.**

    1. Se debe asignar un equipo de trabajo personal e intransferible de uso único y no compartido, ya sea un equipo portátil o de escritorio.

En el momento de la asignación de tareas de monitoreo sobre servidores, almacenamientos, switches, equipos de cómputo y dispositivos de seguridad (cámaras de video, dispositivos de control

1. de acceso), se debe realizar de forma equitativa y que el operador pueda soportar.

2. Realizar la verificación de las actualizaciones para los equipos activos del Datacenter, esta tarea será validada con el administrador de la infraestructura y con el concepto de estabilidad para la actualización por parte del fabricante en la versión más estable, no con esto quiere decir que deba estar con la última actualización libera.

3. Se requiere de la utilización de software de seguridad como son los firewalls definidos por software y que sean de siguiente generación y no convencionales, se recomendara la no utilización de antivirus o antivirus de siguiente generación si no la adquisición de EDR, que son herramientas más robustas y de mejor control que los antivirus, la adquisición de un ambiente de sanbox, donde se realice laboratorio de exploración e investigación de las vulnerabilidades.

- **Establecimiento de los canales de comunicación.**

1. Poseer un sitio WEB o un espacio dentro del portal (micrositio) de la universidad dedicado a la información que estará publicando el **CSIRT-UNAD.**

2. Deberá existir dentro del portal, un área exclusiva para el acceso del personal de seguridad de la información y del **CSIRT-UNAD,** este espacio es de trabajo y acceso controlado y monitorizado.

3. Elaboración de un formulario en línea para el reporte de algún incidente por parte de la comunidad Unadista, ya sean estudiantes, docentes o trabajadores.

4. Correo electrónico exclusivo para cada miembro, correo electrónico general de información, creación de grupos de correo para la recepción y envío de información concerniente a las actividades realizadas día a día y los hallazgos de estas.

5. Se deberá tener una línea telefónica fija, como también la asignación de mínimo dos extensiones dentro del PBX que maneja universidad, se deben contar con una línea celular activa con plan de datos y minutos para uso

exclusivo de los operadores de monitoreo, que reportaran, el estado de la infraestructura o en caso de alguna alerta de ataque elevar las comunicaciones respectivas para la toma de decisiones.

- **Sistema de seguimiento de casos o incidentes.**

1. Sistema de tickets de manejo de incidentes, donde se evidenciará la apertura, respuesta, tiempo de ejecución y cierre de los casos abiertos por generación de vulnerabilidades, aparición de alguna clase de virus informático o ataques, de igual manera esta herramienta deberá tener la capacidad de emitir reportes estadísticos de la información en ella depositada.

- **Varios**.

1. Prever un canal de comunicación alterno en línea, en caso de que las comunicaciones a nombre de la universidad se vean comprometidas.

2. Poseer redundancia de canal de internet con distinto operador en caso de caída de conectividad a internet.

De igual manera y para ir afianzando el plan de acción, se debe tener la información del inventario completo de la infraestructura, como se había mencionado, esto con el fin de identificar y filtrar así que herramientas se seguridad serán aplicadas para la vigilancia.

Plan estratégico de atención de acuerdo a los servicios.

Generación de alertas, advertencias y comunicaciones sobre las vulnerabilidades.

- **Recopilación de información sobre las vulnerabilidades.**

En esta parte, el **CSIRT-UNAD** deberá estar consultando sendas fuentes de información que pueden ser encontradas en los portales WEB de los distintos fabricantes de herramientas para seguridad, de igual manera y como se menciono debe existir el intercambio de información entre diferentes equipos externos a la universidad y llevar un excelente relacionamiento con estos CSIRT.

Esta información llevara al aumento del conocimiento del entorno actual y el afianzamiento del conocimiento general del equipo sobre vulnerabilidades específicas.

Dentro de este plan estratégico se debe tener en cuenta y como se menciona en la recopilación de información de vulnerabilidades, la comunicación y la investigación son fundamentales para generar una buena base de conocimientos y consulta diaria para su operación. Resaltando esto, se debe analizar que el **CSIRT-UNAD**, nace y se madurará de acuerdo con la relevancia que la institución le vaya dando a la aplicabilidad de la seguridad informática, de igual manera son procesos medibles en el tiempo desde su creación hasta una maduración media que podría tardarse entre 12 a máximo 36 meses. Este equipo de trabajo creado y aplicado al plan de actuación, es parte vital para la mitigación de incidentes, debido a ello en la gran mayoría de entidades de educación, cuentan con mesas de ayuda que son en cierto modo ineficaces frente a la respuesta de ataques que estas puedan recibir, esto se deriva a que no se encuentra lo suficientemente estructuradas y no cuentan con el personal calificado e idóneo para responder a estos incidentes.

Es por esto que la cultura de la seguridad debe ser siempre resaltada, administrada y enfocada a medidas proactivas y preventivas y orientadas a la disminución de reactividad.

Por lo anterior, se debe tener a consideración lo siguiente, ¿ante un incidente qué pasa si no se actúa?, esto se responde, a que la pérdida de datos, la violación de los mismos y los daños financieros que conducirán a un daño mayor con implicaciones legales, donde toda la infraestructura física y virtual quedará desactivada e inservible. El tomar medidas, ayuda a resolver los incidentes de manera eficiente y eficaz, y evita tener problemas futuros; no por la presencia de ataques sino en la forma en que se preserva, asegura y respalda la información y la infraestructura. Para esto se debe tener en cuenta lo siguiente

- **Valoración del riesgo y evaluación de la información.**
  En este punto se podrá analizar el impacto de una o varias vulnerabilidades que afectaran la infraestructura de la universidad, teniendo en cuenta niveles de sensibilidad, así: no sensible, sensible, extremadamente sensible. Realizando el análisis de comportamiento de esta, se debe generar una correlación de su existencia frente a otros informes que existan en páginas o fuentes confiables para así determinar si son alertas de falsos positivos (entendido como la detección de un virus o malware no real por parte del antivirus), son vulnerabilidades que puedan generar afectación de los servicios dentro y fuera de la universidad.

Para esto realizamos la descripción de la clasificación de sensibilidad de acuerdo a estándares generales de la industria así:

Tabla 7. Clasificación de Sensibilidad.

CLASIFICACION DE SENSIBILIDAD					
Nivel de sensibilidad	**Definición del nivel de sensibilidad**	**Categorías típicas de incidentes**	**Requerido en las comunicaciones del caso**	**Opcional en las comunicaciones del caso**	**Acceso ITS**
1	Extremadamente sensible.	- Investigaciones globales iniciadas. - Solicitud forense - Destrucción de bienes. - Activo comprometido. - Información comprometida. - Actividad ilícita. - Uso inadecuado de la propiedad. - Violaciones de la política	CSIRT, CPOC	CSIRTM	CSIRT, CSIRTM
2	Sensible.	- Hacking externo - Hacking interno - Acceso no autorizado	CSIRT, CPOC	Operaciones de Seguridad, PROPIETARIOS	Operaciones de seguridad
3	No sensible.	- Denegación de servicio. - Virus / Gusano - Correo electrónico	CSIRT, CPOC	CUALQUIER	TODOS los agentes en ITS

Definiciones:
CPOC: El punto de contacto del cliente, la persona que inició el caso con el CSIRT. Esta es la persona en GI/LP/CIAP que inició un caso con el CSIRT.
CSIRT: Esto incluye a los miembros dedicados de CSIRT y al CSIRT IM que maneja el caso.
CSIRTM: Gerente de Operaciones de Seguridad, Director de Infosec.
Operaciones de seguridad: el grupo Operaciones de seguridad de Infosec. (esto incluye CSIRT y CSIRTM).
PROPIETARIOS: Los propietarios del dispositivo/aplicación afectado (administrador del sistema, webmaster, etc.)
CUALQUIERA: Cualquier otra parte relevante que pueda verse afectada, incluidos varios grupos de empresas. Se deja a la discreción del IM determinar quién
ITS: Sistema de seguimiento de incidentes,

Notas:
** " Comunicaciones de casos" incluyen lo siguiente: correo electrónico inicial de CSIRT al cliente, informes periódicos de casos al cliente e informe final de casos al cliente. No es necesario incluir a estas partes en todas las comunicaciones provisionales que ocurren a lo largo de la vida de un caso, solo las actualizaciones y el resumen del caso.

Fuente 14 Elaboración Propia

- **Relevancia.**

  Es una descripción general del hardware y el software con el que cuenta la universidad y tener en claro por donde se puede a nivel interno generar una utilización para filtrar información de vulnerabilidades. Esto con el fin de generar un ambiente de correlación de herramientas empleadas en otras instituciones para ser probadas y/o buscar alternativas que logren el fin de prevención.

- **Clasificación.**

  De acuerdo a la información adquirida y recopilada, esta debe ser clasificada en ‘restringida’ y de ‘conocimiento público’, esto derivado a que debe existir una política propia de seguridad de la información a nivel interno del **CSIRT-UNAD**, debido a que son registros de análisis de presuntas actividades de ataques, como

también la recopilación de información de sucesos de terceros que pueden afectar la credibilidad e impactar la imagen de una institución o entidad. Debido a lo anterior se genera una clasificación de los incidentes correlacionada a la categorización de sensibilidad antes mencionada y a tener en cuenta así:

Tabla 8. Categorias de Incidentes.

CATEGORIAS DE INCIDENTES		
Categoría de incidente	**Sensibilidad**	**Descripción**
Denegación de servicio	S3	Ataque DOS o DDOS.
Forense	S1	Cualquier trabajo forense a realizar por CSIRT.
Información comprometida	S1	Intento o éxito de destrucción, corrupción o divulgación de información corporativa confidencial o propiedad intelectual.
Activo comprometido	S1, S2	Host comprometido (cuenta raíz, troyano, rootkit),dispositivo de red, aplicación, cuenta de usuario. Esto incluye hosts infectados con malwaredonde un atacante está controlando activamente el host.
Actividad ilegal	S1	Robo / Fraude / Seguridad Humana / Pornografía Infantil. Incidentes relacionados con la informática de naturaleza criminal, probablemente relacionados con la aplicación de la ley, investigaciones globales o prevención de pérdidas.
Hacking interno	S1, S2, S3	Reconocimiento o actividad sospechosa que se origine dentro de la red corporativa de la Compañía, excluyendo el malware.
Hacking externo	S1, S2, S3	Reconocimiento o Actividad Sospechosa originada fuera de la red corporativa de la Compañía (red de socios, Internet), excluyendo malware.
Malware	S3	Un virus o gusano que normalmente afecta a varios dispositivos corporativos. Esto no incluye los hosts comprometidos que están siendo controlados activamente por un atacante a través de una puerta trasera o troyano. (Ver Activo comprometido)
Correo electrónico	S3	Correo electrónico falsificado, SPAM y otros eventos relacionados con la seguridad del correo electrónico.
Consultoría	S1, S2, S3	Consultoría de seguridad no relacionada con cualquier incidente confirmado.
Violaciones de la política	S1, S2, S3	Compartir material ofensivo, compartir/poseer material con derechos de autor.
		Violación deliberada de la política de Infosec.
		Uso inapropiado de activos corporativos como computadoras, redes o aplicaciones.
		Escalada no autorizada de privilegios o intento deliberado de subvertir los controles de acceso.
* - La sensibilidad variará dependiendo de las circunstancias. Se proporcionan directrices.		

Fuente 15 Elaboración Propia

- **Evaluación de riesgos y análisis de impacto.**

Se debe tener en cuenta que el riesgo se define como una posibilidad potencial (probabilidad) que, puede aprovechar una vulnerabilidad, donde se debe tener presente si la vulnerabilidad es conocida, es extendida o es una vulnerabilidad explotable de forma remota, esto con el fin de enfocarse en el cálculo del riesgo de acuerdo a la formula:[78]

Donde el daño se podría potencializar así: acceso no autorizado a los datos, denegación de servicios (DoS) y obtener o extender permisos. Esto se clasifica de acuerdo a la valoración del riesgo en bajo, medio, critico, como ya se mencionó anteriormente y se expone la siguiente tabla de guía según la criticidad del incidente, denotando los tiempos de respuesta guiado de acuerdo a los estándares de la industria:

[78] QUALITY BY DESIGN.EVALUACIÓN DE IMPACTO Y ANÁLISIS DE RIESGOS, ANTES Y DURANTE EL PROCESO DE VALIDACIÓN[En linea]equiere ser validado o para definir el tiempo de revalidación de nuestros sistemas.[Consulta: agosto de 2021]Disponible en:https://www.qbd.lat/evaluacion-de-impacto-y-analisis-de-riesgo/?v=42983b05e2f2

Tabla 9. Clasificación de Criticidad del Incidente.[79]

CLASIFICACION DE CRITICIDAD DEL INCIDENTE						
Nivel de criticidad	**Definición del nivel de criticidad**	**Categorías típicas de incidentes**	**Tiempo de respuesta inicial**	**Respuesta continua (fase crítica)**	**Respuesta continua (fase de resolución)**	**Requisito de comunicación continua**
1	Incidente que afecte a sistemas críticos o información con potencial para ingresos o impacto en el cliente.	- Denegación de servicio	60 Minutos	CSIRT Incident Manager asignado al caso de trabajo las 24x7.	Gerente de Incidentes de CSIRT asignado para trabajar en el caso durante el horario comercial normal.	Actualización del caso enviada diariamente a las partes apropiadas durante la fase crítica. Si la participación de CSIRT es necesaria para restaurar los sistemas críticos al servicio, la actualización del caso se enviará un mínimo de cada 2 horas.
		- Activo comprometido (crítico)				
		- Hacking interno (activo)				Actualización del caso enviada a las partes apropiadas semanalmente durante la fase de resolución.
		- Hacking externo (activo)				
		- Virus / Gusano (brote)				
		- Destrucción de bienes (crítica)				
2	Incidente que afecte a sistemas o información no críticos, no a los ingresos o al cliente. Las investigaciones de los empleados que son sensibles al tiempo generalmente deben clasificarse en este nivel.	- Hacking interno (no activo)	4 Horas	CSIRT Incident Manager asignado al caso de trabajo las 24x7.	Gerente de Incidentes de CSIRT asignado para trabajar en el caso durante el horario comercial normal.	Actualización del caso enviada diariamente a las partes apropiadas durante la fase crítica.
		- Hacking externo (no activo)				
		- Acceso no autorizado.				Actualización del caso enviada a las partes apropiadas semanalmente durante la fase de resolución.
		- Violaciones de la política				
		- Actividad ilícita.				
		- Información comprometida.				
		- Activo comprometido. (no crítico)				
		- Destrucción de bienes (no críticos)				
3	Posibles incidentes, sistemas no críticos. Investigaciones de incidentes o empleados que no son sensibles al tiempo. Investigaciones a largo plazo que involucran una investigación extensa y / o un trabajo forense detallado.	- Correo electrónico	48 Horas	El caso se trabaja ya que el tiempo / recursos de CSIRT están disponibles.	El caso se trabaja ya que el tiempo / recursos de CSIRT están disponibles.	Actualización del caso enviada a las partes apropiadas semanalmente.
		- Solicitud forense				
		- Uso inadecuado de la propiedad.				
		- Violaciones de la política.				

Fuente 16 Elaboración Propia

[79] FIRT.Clasificación de casos CSIRT (ejemplo para CSIRT empresarial)[Sitio web]Es fundamental que el CSIRT brinde una respuesta coherente y oportuna al cliente y que la información confidencial se maneje de manera adecuada.[Consulta: diciembre 2021]Disponible en: https://www.first.org/resources/guides/csirt_case_classification.html

Tabla 10. Definiciones.

DEFINICIONES
Tiempo de respuesta inicial: especifica la cantidad máxima de tiempo que debe transcurre antes de que un administrador de incidentes de CSIRT responda al cliente. Una vez más, esta es la cantidad máxima de tiempo. En la mayoría de los casos, el IM responderá antes del tiempo de respuesta especificado. Como mínimo, lo siguiente debe ocurrir dentro de este período de tiempo:
1. Evaluación inicial y triaje.
2. Se determina la clasificación de los casos.
3. El caso se ingresará en el ITS.
4. Se establecerá la titularidad del caso. (O bien el IM de guardia será el propietario del caso, o se asignará a otro IM).
5. Se enviará un correo electrónico al cliente. Este es el correo electrónico inicial "tenemos su caso". Este correo electrónico incluirá información diversa (que se definirá en otro documento), como la fecha / hora de la solicitud, el número de caso de ITS, el nombre, el teléfono y el correo electrónico del administrador de incidentes, un contacto de escalamiento de CSIRT, el nivel de criticidad y sensibilidad del caso, y una indicación de cuándo el cliente recibirá actualizaciones del caso. Idealmente, el ITS generará este correo electrónico automáticamente cuando se ingrese un caso en el sistema.
Requisito de respuesta continua: especifica el nivel de servicio que el cliente recibirá del CSIRT.
Requisito de comunicación continua: especifica la frecuencia con la que deben producirse las comunicaciones con el cliente a lo largo del ciclo de vida del caso. Estos son los requisitos mínimos, las comunicaciones pueden ocurrir con más frecuencia según sea necesario.

Fuente 17 Elaboración Propia

Tabla 11. Fases del Incidente.[80]

FASES DEL INCIDENTE		
Fase de incidente	**Descripción**	**Actividades típicas**
Fase crítica	El período de tiempo en el ciclo de vida del caso en el que se requiere una respuesta activa a incidentes para garantizar la resolución exitosa del caso. Por lo general, esto incluye interrupciones del sistema o del servicio, y / o preservación urgente de la evidencia.	Detección, evaluación, triaje, contención, preservación de evidencias, recuperación inicial
Fase de resolución	El período de tiempo en el ciclo de vida del caso en el que no se requiere una respuesta activa a incidentes para resolver con éxito el caso.	Recolección de evidencia, análisis e investigación, forense, remediación, recuperación completa, post mortem.
Notas:		
El ITS debe modificarse para incluir una selección desplegable para la fase de incidente ('Crítico','Resolución', 'N/A'). Para los casos que se clasifican como C1 o C2, este campo se establecerá en Crítico cuando se abra el caso y se restablecerá a 'Resolución' en el momento apropiado del ciclo de vida del caso. Para los casos que no son sensibles al tiempo (normalmente C3), el IM establecerá este campo en 'N/A'. Tener esta distinción permitirá que el personal de CSIRT y la administración de operaciones de seguridad distingan fácilmente entre los casos que son críticos y activos de aquellos que no se están trabajando activamente.		

Fuente 18 Elaboración Propia

Distribución de la información.

El **CSIRT-UNAD**, deberá elegir el medio o el método de comunicación y distribución de la información de acuerdo a la estrategia de comunicación propuesta por el designado de comunicaciones dentro del equipo de trabajo, esto debe contar con la aprobación del **CISO** (Chief Information Security Officer), para

[80] FIRT.Clasificación de casos CSIRT (ejemplo para CSIRT empresarial)[Sitio web]Es fundamental que el CSIRT brinde una respuesta coherente y oportuna al cliente y que la información confidencial se maneje de manera adecuada.[Consulta: diciembre 2021]Disponible en: https://www.first.org/resources/guides/csirt_case_classification.html

esto se podría optar por sitio web, correo electrónico, informes y archivo e investigación, los comunicados y el manejo de la información siempre deberán ir en un mismo formato, que debe ser aprobado por el sistema de gestión de calidad y formatos del sistema de gestión y seguridad de la información.[81]

- **Manejo de incidentes.**
  Para manejo de incidentes, se debe realizar un procedimiento muy similar al de recolección de información sobre alertas, advertencias, indicios de falsos positivos, en el inicio de cualquier acción siempre se debe generar inmediatamente un caso identificado con numero de ticket y realizando una descripción detallada de la situación.

[81] FIRT.Clasificación de casos CSIRT (ejemplo para CSIRT empresarial)[Sitio web]Es fundamental que el CSIRT brinde una respuesta coherente y oportuna al cliente y que la información confidencial se maneje de manera adecuada.[Consulta: diciembre 2021]Disponible en: https://www.first.org/resources/guides/csirt_case_classification.html

Formato de reporte de incidentes.

REPORTE DE INCIDENTES																	
NUMERO DE REFERENCIA										FECHA	D	D	M	M	A	A
DATOS DEL REPORTANTE																	
NOMBRE Y APELLIDO																	
CEDULA																	
NUMERO DE TELEFONO/CELULAR																	
CORREO ELECTRONICO																	
CARGO																	
SEDE/REGIONAL																	
DEPENDENCIA/FACULTAD																	
CIUDAD																	
DESCRIPCION HARDWARE/SOFTWARE AFECTADO																	
SERVIDORES		ALMACENAMIENTO				SWITCHES				DESKTOP/LAPTOP							
NOMBRE DEL HOST - IP																	
FUNCION DEL HOST																	
COBFIGURACION DEL HARDWARE AFECTADO (Descripcion de componentes internos - Raid, si aplica)																	
SISTEMA OPERATIVO - COMPILACION																	
SOFTWARE AFECTADO																	
ARCHIVOS AFECTADOS (DATA - BASES DE DATOS)																	
SISTEMA DE SEGURIDAD EMPLEADO (ANTIVIRUS-EDR-FIREWALL)																	
PROTOCOLO - PUERTO(S) AFECTADOS																	
TIPO DE INCIDENTE																	
INCIDENTE INICIADO (DESCRIPCION DEL COMPORTAMIENTO, SINTOMAS, HORA DE INICIO)																	
INCIDENTE CONTINUO		SI		NO													
MOMENTO Y METODO DE DESCUBRIMIENTO (ALERTAS GERADAS - DESCRIPCION)																	
VULNERABILIDADES CONOCIDAS																	
ARCHIVOS SOSPECHOSOS																	
CONTRAMEDIDAS																	
DESCRIPCION DETALLADA DEL INCIDENTE																	

Formato de seguimiento recopilación de información e inicio de atención a incidentes

UNAD Universidad Nacional Abierta y a Distancia

AVISO INFORMATIVO	ACCESO RESERVADO						SI	NO	ACCESO PUBLICO					SI	NO
NUMERO DE REFERENCIA							FECHA		D	D	M	M	A	A	

SISTEMAS AFECTADOS
Descripcion

Version de Sistema Operativo	Compilacion

RIESGO	Alto	Medio	Bajo

Descripcion

Impacto/Daño Potencial	Alto	Medio	Bajo

Identificacion Externa		SI			NO	

Descripcion del Boletin

Identificacion Interna		SI			NO	

Descripcion del Boletin

Descripcion General de la Vulnerabilidad

Descripcion del Impacto

Descripcion de la Solucion

Cabe recalcar que la información de incidentes debe llegar al **CSIRT-UNAD**, por medio de correo electrónico, llamada o a través de una herramienta de gestión que puede ser la que use la mesa de ayuda, como por ejemplo Aranda o GLPI.

Se debe realizar un análisis inmediato y comprobación de su autenticidad y relevancia para su clasificación de afectación. Dentro de la identificación por buena práctica se debe corroborar la autenticidad de la fuente, que está realizando la denuncia de la posible vulnerabilidad o ataque en curso, debido a lo anterior se refleja la relevancia, que esta va a tener. Es decir, una generación real de amenaza o simplemente se cataloga como una ataque fallido o falso positivo.

La clasificación de la gravedad de un incidente, se debe mediar a la valoración de acuerdo a un procedimiento médico que es aplicable a varias áreas del conocimiento, conocido como TRIAGE (la valoración del paciente para clasificar el nivel de servicio de atención en urgencia), esta actividad debe ser de carácter obligatorio debido a que es el paso fundamental de clasificación hacia un camino de atención critica o simplemente el levantamiento de una advertencia o alerta de cuidado, esta actividad debe ser acompañada por parte del **SOC** y el **NOC** y el **CSIRT-UNAD** será el encargado único de contacto en medio de una crisis, esto permite que se genere un análisis, evaluación y clasificación de un caso entrante, esto proporciona una visión clara y en tiempo real de la situación para tomar acciones, como el traslado de las operaciones al Datacenter alterno o bajar todos los servicios e iniciar los programas de DRP o PLD.

- **Ejecución de acciones.**

  Para esta ejecución se deberá tener en cuenta la utilización de una herramienta de gestión que antes fue mencionado; como el ejemplo de Aranda o GLPI, que permita la generación de tickets de atención no solo para la mesa de ayuda sino para el grupo de seguridad de la información como el **CSIRT-UNAD**, esto permitirá la gestión, trazabilidad, análisis, encolamiento y ejecución de la atención de incidentes.

  Una vez creado el incidente dentro de la herramienta de gestión, deberemos valorar el ciclo de vida del incidente, esto con el fin de llegar a solución y tener documentado todo el historial del caso, para esto se debe tener en cuenta los siguientes pasos:

1. **Análisis:** se realiza un análisis de la información plasmada en el caso de apertura del ticket, para esto se debe tener en cuenta que se solicita una descripción detallada de lo sucedido o de la acción que está en ejecución.

2. **Información del contacto:** se recopilará la información y se tomará contacto con quien reporta, para realizar una cadena de seguimiento de las personas, dependencias y/o servicios involucrados en el incidente para evaluar los sistemas comprometidos en el incidente, vulnerabilidad o ataque.

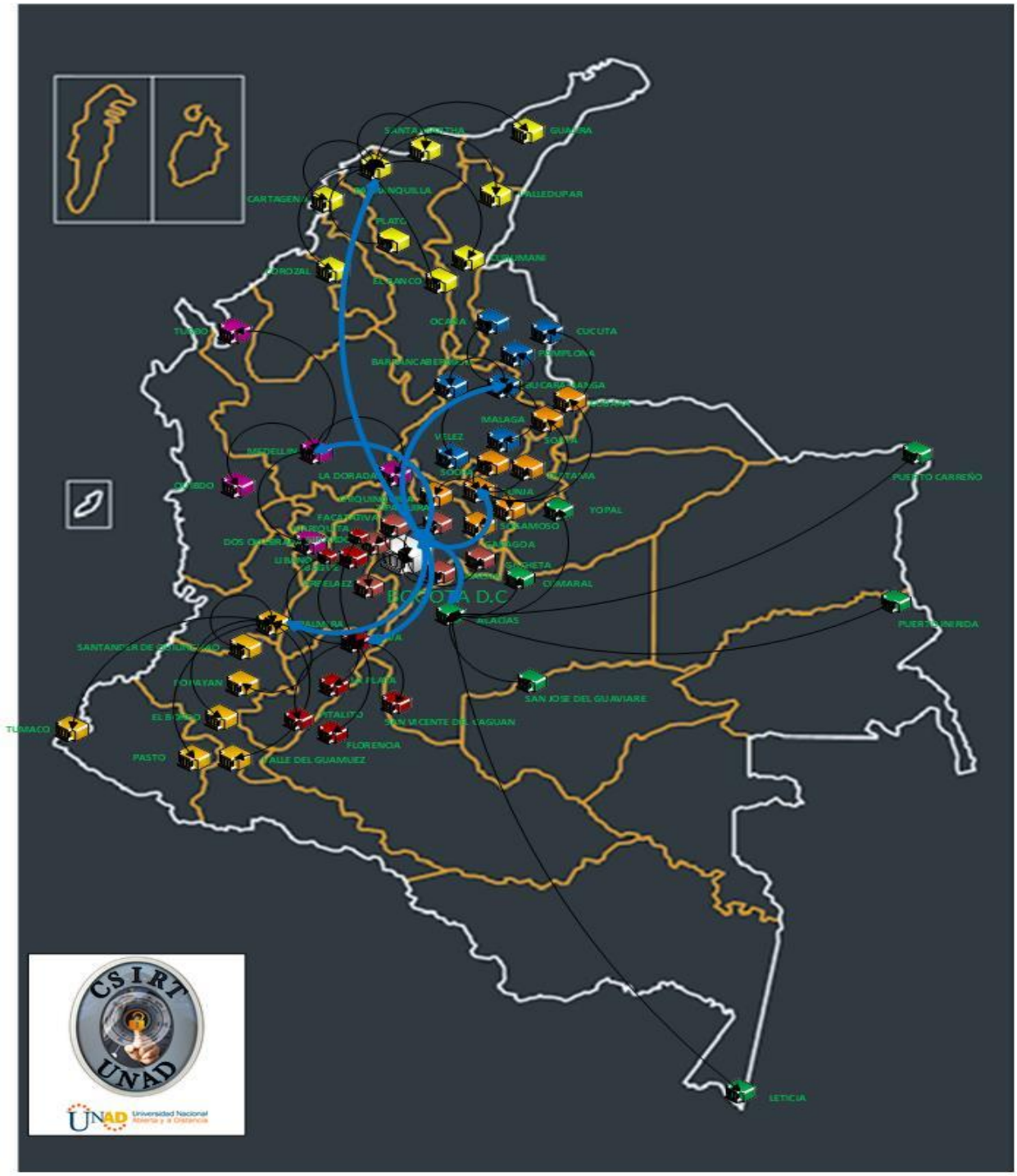
3. **Soporte técnico:** se debe tomar acción inmediata, activando el o los planes de DRP o PDL y generando un aislamiento de la víctima del incidente y proveer un plan de recuperación tratando de llegar al mínimo impacto de perdida de datos o suspensión del servicio, esto se aplica al principio técnico de continuidad de negocio.

4. **Coordinación:** parte esencial de la cadena de atención, porque esta será la parte de atención, análisis, toma de decisiones, análisis post incidente, recopilación de la lección aprendida, comunicación estratégica y archivado de las memorias del caso.

5. **Informe del incidente:** este material se debe preparar de dos formas, un informe detallado de la acción del incidente en caso de que se necesite presentar una acción legal y las autoridades soliciten una descripción detallada de lo sucedido y otro un informe ejecutivo, donde se explique a la rectoría de lo sucedido, resumiendo en clase de incidente, acciones tomas y soluciones provistas y medidas de remediación.

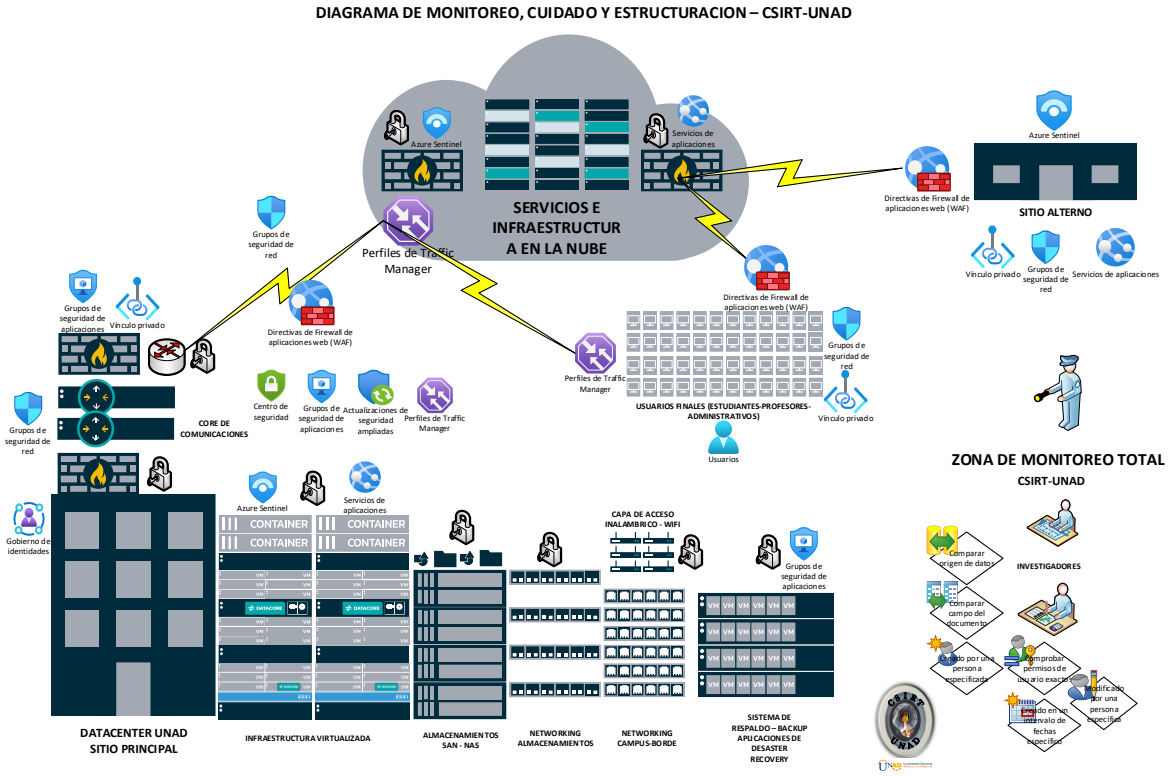
6. **Archivado del incidente:** se debe contar con un archivo digital y en custodia del área del sistema de seguridad de la información, de toda la trazabilidad del caso atendido, como también del paso a paso de las acciones tomadas con el fin de poseer información de consulta en caso de haber repetibilidad del incidente, como también en caso de inspecciones con orden judicial.

Figura 13 Sistema Sugerido de Interconexión y seguridad de red.



Fuente 19 Elaboración Propia

Figura 14 Diagrama de monitoreo, ciudad y estructuración CSIRT-UNAD.



Fuente 20 Elaboración Propia

10. CONCLUSIONES

Las nuevas políticas y controles que establece la norma ISO 27001:2013, con relación a la ISO 27001:2005, nos ayudó a realizar la propuesta de actualización de los controles y políticas en la Universidad nacional Abierta y a Distancia, para fortalecer la seguridad de la información de las mismas e implementar un Csirt- Unad.

Frente a la propuesta investigativa se logra resolver la pregunta problema a partir de una implementación completa del Csirt UNAD donde se abarcaron los puntos clave y estratégicos que componen a una constitución de seguridad. En este sentido se tomó en cuenta la triada de ciberseguridad: la confidencialidad, integridad y disponibilidad que, contribuyeron al análisis de las circunstancias negativas que podría tomar lugar dentro del plantel educativo si no se consideran medidas frente a la protección y conservación de la información universitaria.

En este orden de ideas, con la aplicación de los controles de la seguridad de la información teniendo en cuenta la norma ISO 27001:2013, se logra la actualización de los ya adoptados por la UNAD basados en la norma ISO 27001:2005, lo que nos permite adaptarnos a la evolución de los nuevos riesgos, minimizando estos de forma permanentemente, realizando las adecuaciones pertinentes para mantener la certificación en dicha norma.

Se diseña un esquema de ciberseguridad para el Centro de Respuesta a Incidentes informáticos, donde se destaca el estado actual de las políticas, procesos y procedimientos relacionados con la seguridad de la información dentro del plantel universitario. De este modo, se garantiza un apoyo directo al mejoramiento de las aplicaciones de las actividades en los centros de seguridad para mantenimiento y vigilancia de la información de la Universidad Nacional Abierta y a Distancia UNAD.

Se establece la estructura de responsabilidades y funciones relacionadas con el área de tecnologías de la información, donde las competencias y conocimientos se dividen en subáreas que tratan las prioridades de los incidentes que permiten el control y previa solución de estos.

Se documenta el estado actual de las políticas, procesos y procedimientos de la Universidad, observando las transformaciones de estas para la actualización designada a la consolidación de una normativa que vaya de la mano con la protección de la información en conjunto de una implementación CSIRT.

Se propone una organización innovadora en la que se incluye roles, responsabilidades y funciones del Centro de Respuesta a Incidentes informáticos, que por medio de un estatuto compila las actividades y competencias para la implementación adecuada para la resolución de incidentes dentro de la universidad.

Se formula un plan estratégico para la atención de eventos cibernéticos, que contrastan la reacción y solución de posibles ataques a la información con una coordinación interna en el área de TI.

11. RECOMENDACIONES

Actualizar la declaración de aplicabilidad con las políticas y controles propuestos, los cuales están basados en la norma ISO 27001:2013, realizando para ello la respectiva difusión de la misma, al igual que la elaboración e implementación de las nuevas políticas para la conformación del Csirt- Unad.

Adoptar una cultura seguridad de la información dentro de la organización para así difundir, afianzar y aplicar las políticas de cuidado y preservación de la información.

Crear un equipo que cuente con miembros capacitados en seguridad informática que actúen de manera reactiva a los incidentes que se presenten, respetando la normativa de roles y funciones para el cumplimiento de los procesos y procedimientos.

Aplicar las políticas y controles propuestos, con el fin de minimizar riesgos y fortalecer los controles de acceso, transporte y almacenamiento de los activos de información de la UNAD.

12. DIVULGACIÓN

El desarrollo del presente proyecto de grado será dado a conocer en colaboración de la biblioteca de la Universidad Nacional Abierta y a Distancia – UNAD, a través de su aplicativo en línea, en donde se publicará un archivo PDF correspondiente al documento final presentado ante los jurados, posterior a la sustentación de este; con el fin de que todos los estudiantes de la Universidad que se encuentren interesados en el tema del estado actual de las políticas, procesos y procedimientos relacionados con la seguridad de la información de la Universidad Nacional Abierta y a Distancia UNAD, con un Centro de Respuestas a Incidentes Informáticos (CSIRT-UNAD), puedan acceder al documento.

BIBLIOGRAFÍA

- ANAPUR. (s.f.). CYBER-SICHERHEITSSTRATEGIE 2021;Cyber-Sicherheitsstrategie 2021 des BMI[Sitio web]La estrategia de ciberseguridad para Alemania forma el marco del gobierno federal para sus actividades en el área de ciberseguridad [Consulta: 14 Abril de 2021]Disponible en. Obtenido de https://anapur.de/cyber-sicherheitsstrategie-2021-eckpunktepapier-des-bmi-jetzt-stellung-nehmen

- ASOBANCARIA. (s.f.). Un enfoque colaborativo a la Ciberseguridad[Sitio web]equipo colaboración para mitigar riesgos derivados de amenazas[Consulta: 2019]Disponible en:. Obtenido de https://www.asobancaria.com/csirt/

- BARRIOS ACHAVAR, V. (s.f.). Política Nacional de Ciberseguridad: 2017-2022[En linea]La revolución que ha vivido el denominado ciberespacio[Consulta:Julio de 2018]Disponible en:. Obtenido de https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/26760/1/POLITICA_NACIONAL_DE_CIBER.pdf

- CANO VARGAS, J., & línea], [. ([2020]). Propuesta de los documentos administrativos para la Creación de un Centro de Respuesta a Incidentes Cibernéticos para la empresa caso de estudioCibersecurity de Colombia LTDA. Disponible en. Obtenido de https://repository.unad.edu.co/bitstream/handle/10596/36488/jjcanov.pdf?sequence=1&isAllowed=y

- CENTRO NACIONAL DE CONSULTORIA. (s.f.). revela estudio de apropiación digital en Colombia[Sitio web]BOGOTÁ [Consulta: 7 diciembre de 2017]Disponible en:. Obtenido de https://www.centronacionaldeconsultoria.com/post/2017/12/07/centro-nacional-de-consultor%C3%ADa-revela-estudio-de-apropiaci%C3%B3n-digital-en-colombia

- COLCERT. (s.f.). Grupo de Respuesta a Emergencia Cibernetícas de Colombia[www.colcert.gov.co][Sitio web]organismo coordinador a nivel nacional en aspectos de ciberseguridad y ciberdefensa del Estado[Consulta: Enero 2021]Disponible en:. Obtenido de https://www.colcert.gov.co/

- COLEGIO OFICIAL DE INGENIEROS DE TELECOMUNICACIÓN,. (s.f.). Implantación de Sistemas de Gestión de la Seguridad de la Información (SGSI) [En linea]según la norma ISO 27001[Consulta: 15 abril de 2012]. Obtenido de https://www.coit.es/sites/default/files/informes/pdf/implantacion_de_sistemas_de_gestion_de_la_seguridad_de_la_informacion_sgsi_segun_la_norma_iso_27001.pdf

- COVIX, G. (s.f.). Seguridad Física[Sitio web] Para esto es necesario aplicar barreras físicas y procedimientos de control como medidas de prevención y contramedidas ante amenazas a los recursos.[Consulta: 2018]Disponible en:. Obtenido de https://www.grupocovix.com/pages/seguridad-fisica

- DEFENSE ADVANCED RESEARCH PROJECTS AGENCY. (s.f.). Creando innovadoras tecnologias y capacidades por la seguridad nacional [www.darpa.mil]; [Consulta: 20 de Julio de 2021]. Disponible en:. Obtenido de https://www.darpa.mil/

- FIRT. (s.f.). Clasificación de casos CSIRT (ejemplo para CSIRT empresarial)[Sitio web]Es fundamental que el CSIRT brinde una respuesta coherente y oportuna al cliente y que la información confidencial se maneje de manera adecuada.[Consulta: diciembre 2021]Disponible en. Obtenido de https://www.first.org/resources/guides/csirt_case_classification.html

- FORTINET. (s.f.). www.fortinet.com,Next-Generation Firewall (NGFW)[Sitio Web]el filtrado de paquetes, la compatibilidad con IPsec y VPN SSL[Consulta 2021] Disponible en:. Obtenido de https://www.fortinet.com/lat/products/next-generation-firewall

- GAVIRIA ALVAREZ, W. (27 de Septiembre de 2017). Propuesta de actualización de Políticas de Seguridad de la Información del Sistema de Gestión de la Información de la Empresa Caso de Estudio, en la Sede Medellín de la ISO 27001:2005 a la ISO 27001:2013. Obtenido de https://repository.unad.edu.co/handle/10596/13274

- GOBIERNO DIGITAL. (s.f.). ¿QUÉ ES EL CSIRT GOBIERNO?[Sitio web]El CSIRT del sector Gobierno, surge como necesidad de realizar una adecuada gestión y reaccionar ante los incidentes cibernéticos[Consulta: 2021]Disponible en:. Obtenido de https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/CSIRT-Gobierno/

- GONZALEZ, P., SANCHEZ, G., & SORIANO, J. (s.f.). OXWORD;Pentesting con Kali Silver Edition[Sitio web]libros de seguridad Informatica[Consulta: Agosto 2020]Disponible en:. Obtenido de https://0xword.com/es/libros/40-libro-pentesting-kali.html

- INCIBE. (s.f.). Gestión de Riesgo[En línia]Una guia de aproximación para el empresario[Consulta: dic 2021]Pag. 4 a la 8Disponible en:. Obtenido de https://www.incibe.es/extfrontinteco/img/File/empresas/guias/Guia_gestion_riesgos/guiagestionriesgos.pdf

- IONOS. (s.f.). Gestión de crisis: cómo afrontar situaciones de emergencia[Sitio web]las empresas que se encuentran en una buena situación también pueden

verse afectadas por acontecimientos imprevistos que amenacen su existencia.[Consulta: 29 abril de 2020]Disponible en:. Obtenido de https://www.ionos.es/startupguide/gestion/gestion-de-crisis/

- ISO 31000, . (s.f.). GESTIÓN DE RIESGOS;[Sitio web].evaluar y actualizar continuamente su oferta hasta optimizar sus procesos.[Consulta: octubre 19 2021]Disponible en:. Obtenido de https://www.iso.org/iso-31000-risk-management.html

- ISO/IEC:27001. (s.f.). Referencias normativas en las que está basada la norma ISO 27001.Segunda Edicion[Sitio web][normaiso27001.es][Consulta: 15 de Junio 2005]Disponible en:. Obtenido de https://normaiso27001.es/referencias-normativas-iso-27000/

- ISOTOOLS. (s.f.). La familia de normas ISO 27000.[www.isotools.org][Sitio web]Esta estandarización contiene las definiciones y los términos que se utilizarán durante toda la serie 27000.[Consulta: 21 de Enero de 2015] Disponible en:. Obtenido de https://www.isotools.org/2015/01/21/familia-normas-iso-27000/

- ITMASTERSMAG. (s.f.). El estado de la seguridad IT en 2020:[www.itmastersmag.com] Las superficies de ataque se amplían y las personas nunca fueron tan importantes para la defensa[Sitio web],[Consulta: 2021]Disponnible en:. Recuperado el 08 de Octubre de 2020, de https://itmastersmag.com

- LEIVA JIMENEZ, J., & CHIARI CABALLERO, J. (s.f.). Implementación de la fase inicial de un sistema de gestion de la seguridad de la información en el grupo de TI de una entidad del sector publico colombiano[En Linea].monografia[Consulta: 2013]Disponible en:. Obtenido de http://polux.unipiloto.edu.co:8080/00001038.pdf

- LISOT. (2021). Principios de la seguridad informática: Confidencialidad, Integridad y Disponibilidad de la información. [www.lisot.com] Disponible en. Obtenido de https://www.lisot.com/que-es-un-sistema-de-gestion-de-la-seguridad-de-la-informacion-sgsi/

- LOTERIA NACIONAL PARA LA ASISTENCIA PUBLICA, . (s.f.). MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN[En linea]Pag 5-10[Consulta: Octubre de 2018]Disponible en:. Obtenido de https://www.gob.mx/cms/uploads/attachment/file/508072/M_SISTEMA_GESTION_SEGURIDAD_INFORMACION_Parte1.pdf

- MINISTERIO DE EDUCACIÓN NACIONAL. (s.f.). Plan estratégico de de tecnologias de la información 2019/2022[En linea]gestionar los recursos de tecnología de la información[Consulta: Enero de 2019] Disponible en. Obtenido de https://www.mineducacion.gov.co/1759/articles-362792_galeria_11.pdf

- MINISTERIO DE LAS TECNOLOGIAS DE INFORMACIÓN TIC. (2021). Guía para la Implementación de Seguridad de la Información en una MIPYME. seguridad de la información,[En Línea] [Consulta: noviembre de 2021], Disponible en:. Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

- NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. (s.f.). NIST, [Sitio web],Trabajar con la industria y la ciencia para promover la innovación y mejorar la calidad de vida.[Consulta: 2019]Disponible en:. Obtenido de https://www.nist.gov/

- OCHOA CASTAÑEDA, J. (s.f.). Propuesta de la Creación de políticas de seguridad para Cormagdalena[En Linea]mplementar un excelente esquema de políticas de seguridad[Consulta: 7 de mayo de 2018]Disponible en:. Obtenido de https://alejandria.poligran.edu.co/handle/10823/1227

- PERIODISTA DIGITAL . (s.f.). El Gusano Morris y los daños que causó en Internet [Sitio web], [Consulta: 16 de julio de 2019]. Disponble en:]. Obtenido de https://www.periodistadigital.com/tecnologia/tec-internet/20190726/gusano-morris-danos-causo-internet-noticia-689404036001/

- PORTAL DE AMINISTRACIÓN ELECTRÓNICA. (s.f.). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información[Sitio web][Consulta: Octubre de 2012]Disponible en:. Obtenido de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.YaDuhbq23IU

- POWERDATA. (s.f.). www.powerdata.es[Sitio web]Seguridad de datos: En qué consiste y qué es importante en tu empresa.[Consulta: agosto 2 de 2021] Disponible en:. Recuperado el 3 de Diciembre de 2020, de https://www.powerdata.es/seguridad-de-datos

- QUALITY BY DESIGN. (s.f.). EVALUACIÓN DE IMPACTO Y ANÁLISIS DE RIESGOS, ANTES Y DURANTE EL PROCESO DE VALIDACIÓN[En linea]equiere ser validado o para definir el tiempo de revalidación de nuestros sistemas.[Consulta: agosto de 2021]Disponible en:. Obtenido de https://www.qbd.lat/evaluacion-de-impacto-y-analisis-de-riesgo/?v=42983b05e2f2

- SAIZ, J. (s.f.). Matriz de evaluación de riesgos. Un sistema de valoración[Sitio web]La matriz de evaluación de riesgos te permite realizar un análisis cuantificable de los riesgos en tus proyectos. Te explico cómo hacerla.[Consulta: 30 de abril de 2020]Disponible en:. Obtenido de https://jorgesaiz.com/blog/matriz-de-evaluacion-de-riesgos/

- SCSCONSULTING. (s.f.). ISO 27001:2013 Sistema de gestion de seguridad de la Información (SIGS) [www.scsconsulting.es][Consulta: 2020]Disponible en:. Obtenido de https://www.scsconsulting.es/iso-27001-2013-sistema-de-gestion-de-seguridad-de-la-informacion/

- SECURESOFT , C. (s.f.). ¿Cómo organizar un CSIRT?Un equipo de respuesta a incidentes de seguridad informática (CSIRT) puede ayudar a mitigar el impacto de las amenazas a la seguridad de cualquier organización[Sitio web],[consulta: 20 de julio de 2018] Disponible en:. Obtenido de https://securitysummitperu.com/articulos/como-organizar-un-csirt/

- SECURITY, H. (s.f.). La seguridad cibernética[Sitio web]Para promover el compromiso del presidente y para reflejar que mejorar la resiliencia de la seguridad cibernética de la nación es una prioridad principal para el DHS[Consulta: 22 Octubre 2021]Disponible en:. Obtenido de https://www.dhs.gov/topic/cybersecurity

- SECURITYSCORECARD. (s.f.). www.securityscorecard.com. Recuperado el [2018], de Informe sobre ciberseguridad en la educación 2018.[Sitio web]Los resultados muestran que, aunque los piratas informáticos se han vuelto cada vez más hábiles para robar datos de escuelas y estudiantes[Consulta: 2020] Disponible en:: https://securityscorecard.com/resources/2018-education-report

- SERPOLSOFT. (s.f.). software para seguimiento de casos e incidentes[Sitio web]APROWEB es la aplicación web más fácil de usar para ayudar a su empresa a mejorar el servicio hacia sus clientes.[Consulta: 2020]Disponible en:. Obtenido de https://www.serpol.net.mx/casos

- SLIDESERVER. (s.f.). Gestión de la Seguridad de la Información según ISO/IEC 17799.[www.slideserve.com] Objetivo de la Ponencia Situación Actual de las TIC Definiciones Importancia de la Seguridad[Consulta: 11 nov 2021]Disponible en:. Obtenido de https://www.slideserve.com/yoshiko/gesti-n-de-la-seguridad-de-la-informaci-n-seg-n-iso

- SYNNEX. (s.f.). LAS 10 MEJORES PRÁCTICAS DE SEGURIDAD DE LA INFORMACIÓN[Sitio web]Descubre puntos importantes a tener en cuenta cuando se trata de proteger su negocio.[Consulta: 26 febrero de 2016]Disponoble en:. Obtenido de http://digital.la.synnex.com/las-10-mejores-practicas-de-seguridad-de-la-informacion

- TELECOMUNICACIONES. (s.f.). CCTI Camara Colombiana de Informatica y Tendencias del Cibercrimen en Colombia 2019-2020[Sitio web][Consulta: Octubre de 2019]Disponible en:. Obtenido de https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

- UNAD. (© Copyright UNAD 2021). Política de seguridad de la información y gestión documental. Obtenido de Por la cual se definen las políticas del Marco de Referencia del SGSI: https://sgeneral.unad.edu.co/sistema-de-gestion-documental/normatividad-gestion-documental/politica-de-seguridad

- UNESCO. (s.f.). Declaración mundial sobre la educacion superior en el siglo XXI: Visión y Acción[www.iesalc.unesco.org] Disponible en:. Recuperado el 20 de Agosto de 2019, de https://www.iesalc.unesco.org/ess/index.php/ess3/article/view/171

- UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. (2 de Febrero de 2018). Plan Estratégico de Seguridad y Privacidad de la Información GIDT-PTI. Disponible en. Obtenido de https://gidt.unad.edu.co/images/Documentos/Plan-de-Seguridad-y-Privacidad-de-la-Informacion.pdf

- UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. (12 de Enero de 2020). Plan Estrategico de Tecnologia de información de la UNAD [En Línea] Disponible en:. Obtenido de https://gidt.unad.edu.co/images/Documentos/PLAN_ESTRATEGICO_DE_TECNOLOGIAS_DE_LA_INFORMACION_UNAD_Vr7.pdf

- UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. (2021). Gerencia de Innovación y Desarrollo Tecnológico Organigrama PTI [Sitio web] [Consulta: en el 2020]. Disponible en:. Obtenido de https://gidt.unad.edu.co/acerca-de/organigrama

- UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. (s.f.). UNAD;Acerca de la Transparencia y Acceso a la Información Pública[Sitio web]La Universidad Nacional Abierta y a Distancia (UNAD) tiene como misión contribuir a la educación para todos a través de la modalidad abierta.[Consulta: 2021]Disponible en:. Obtenido de https://informacion.unad.edu.co/

- UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA[Sitio web]. (s.f.). [gidt.unad.edu.co] Seguridad de la información Principios básicos de Seguridad Informática y de la Información. Disponible en. Recuperado el [2020], de https://gidt.unad.edu.co/seguridad-de-la-informacion

- UPTIME, I. (s.f.). Sistema de clasificación Tier[Sitio web]los niveles de Tier Classification de centros de datos hace más de 25 años, y hoy en día siguen sel estándar internacional para evaluar el desempeño de un centro de datos.[Consulta: 2020]Disponible en:. Obtenido de https://es.uptimeinstitute.com/tiers

- WELIVESECURITY. (s.f.). ¿Qué es y cómo trabaja un CSIRT para dar respuesta a incidentes?[Sitio web]Los equipos de respuesta a incidentes de seguridad

(CSIRT) buscan restituir las actividades con el impacto mínimo.[Consulta: 18 de mayo de 2015]Disponible en:. Obtenido de https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/

- ZAMBRANO HERNANDEZ, F. (2021). Buenas prácticas para establecer un CSIRT nacional Semilleros Ceros y Unos [Consulta: Agosto de 2021], [Disponible en:]. Obtenido de https://semillerocerosyunos.com/index.php/2021/07/02/buenas-practicas-para-establecer-un-csirt-nacional/

ANEXOS

Anexo A. Nombre del Anexo

Anexo B. Nombre del Anexo