Diseño del Sistema de Gestión de Seguridad de la Información (SGSI) para una Universidad

Edwin González Torres
Weimar Gutierrez Garcia
Departamento de Ingeniería de Sistemas y ComputaciónUniversidad de los Andes
e.gonzalezt@uniandes.edu.co
w.gutierrez@uniandes.edu.co

Resumen

Este artículo describe cómo realizar el diseño exitoso de un SGSI para una institución educativa odontológica, teniendo como base el ciclo PHVA y la norma ISO27003.

Basados en los antecedentes de la organización se ha optado por realizar una serie de sesiones técnicas de entendimiento con la institución con el fin de obtener de una forma clara la situación actual de la organización, a partir de lo anterior se ha decido llevar a cabo un plan de diseño técnico herramental y otro enfocado hacia procesos internos de la organización, que involucre procesos y procedimientos nuevos dentro de la organización, finalmente la implementación de un plan piloto que involucre análisis de vulnerabilidades y amenazas actuales y el valor agregado para el negocio.

Abstract

This article describes how to carry out the successful design of an ISMS for a dental educational institution, based on the PHVA cycle and the ISO27003 standard.

Based on the background of the organization, it has been decided to carry out a series of technical sessions of understanding with the institution in order to obtain clarity on the current situation of the organization, based on the above, I decide to carry out a design plan. technical tooling and another focused on internal processes of the organization, which involves new processes and procedures within the organization, finally the implementation of a pilot plan that involves analysis of vulnerabilities and current threats and added value for the business.

I. CONTEXTO

A. *Antecedentes del Problema*

La universidad no cuenta con un área o grupo para el manejo de incidentes. A pesar de que existe un grupo operando la seguridad de la red, los incidentes no son documentados y no hay un correcto manejo de estos para solventarlos. En el año 2019 la universidad realizo una auditoría externa para identificar vulnerabilidades en las estaciones de trabajo (computadores de escritorio y portátiles) y la identificación de Malware que pudiera estar presente en los equipos. Como resultado de la auditoria, La universidad decidió implementar un controlador de dominio que permitiera centralizar el acceso a los recursos y tener un control de identidad para reducir las vulnerabilidades.
Desde la creación del datacenter y la implementación de la infraestructura tecnológica en la universidad, ésta no ha implementado ningún sistema de monitoreo y gestión de sus activos tecnológicos, lo cual ha evitado el correcto control del estado de salud, la identificación de fallas, vulnerabilidades e identificación de ciberataques.

Dada la contingencia del COVID-19 para la universidad, se convirtió en prioridad prestar sus servicios a través de medio digitales, principalmente sus clases, servicios de consulta de libros, archivos digitales e historias clínicas de carácter sensible. Es importante mencionar que actualmente los registros médicos se encuentran anonimizados y de esta manera pueden ser consultados por los estudiantes, no obstante, el departamento de TICs (Tecnologías de la Información) desea aplicar nuevos controles para garantizar su seguridad. Por la misma razón, la universidad reforzó sus tecnologías mediante el despliegue de sus servicios en una nube privada, nuevos

canales de soporte técnico como email y soporte telefónico para estudiantes y profesores, y la creación de nuevos portales para la consulta de documentos los cuales deben estar disponibles 24/7.

Se selecciona la norma ISO27003 dado que brinda una orientación para lograr un diseño exitoso del SGSI, así como requisitos de la norma ISO27001.
Basados en la norma ISO 27003, y con el fin de generar de manera exitosa el diseño del SGSI para la organización, se llevarán a cabo cada una de las actividades establecidas dentro del cronograma general de diseño del proyecto.
Debido a que la universidad no ha tenido acercamiento con las normas ISO 27000 se creará un sistema de gestión de seguridad de la información, de igual forma se entregará un prototipo para el monitoreo de la infraestructura alojada en el datacenter y una herramienta de análisis de vulnerabilidades, estos prototipos nos permitirán evidenciar el estado actual de la organización en cuanto a seguridad, y al compararlos, se evidencia un enfoque desalineado con los controles y políticas de la institución actuales. Con el fin de evidenciar el cambio en la organización y poder medir la efectividad del diseño propuesto, se realizarán los correspondientes indicadores de gestión y de implementación que nos darán el antes y el después, dando la posibilidad de observar el valor agregado que como proyecto y objetivo del mismo se desea conseguir, evidenciando el cambio en la organización y posterior contribución a la mejora de los procesos e impacto real positivo organizacional.

B. Justificación del Problema

Uno de los blancos que han sido atacados constantemente en los últimos años por los ciberdelincuentes son las entidades educativas ya que el grupo de víctimas y afectados es muy amplio. El IC3 (Internet Crime Complaint Center) en su Internet Crime Report del 2021 (IC3, 2021), informa que se generó una advertencia gracias a los reportes del FBI (federal bureau of investigation) donde se expone el aumento del uso del ransomware PYSA dirigido a instituciones educativas. Por otro lado, en un informe conjunto del FBI, CISA (Cybersecurity and Infraestructure Security Agency) y el MS-ISAC (Multi-State Information Sharing and Analysis Center), se indica que los ciberdelincuentes tienen como objetivo las instituciones educativas, provocado ataques de ransomware, el robo de datos y la interrupción de los servicios de aprendizaje a distancia. Adicional, en este informe se resalta que el 57% de los ataques de ransomware entre agosto y septiembre de 2020 fueron contra las entidades educativas según los datos del MS-ISAC. (Cybersecurity & Infrastructure Security Agency, 2020)
En la siguiente imagen se observa los 10 principales programas maliciosos que atacan a las instituciones educativas:

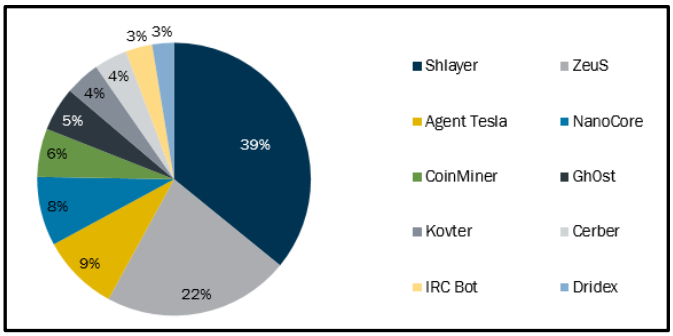
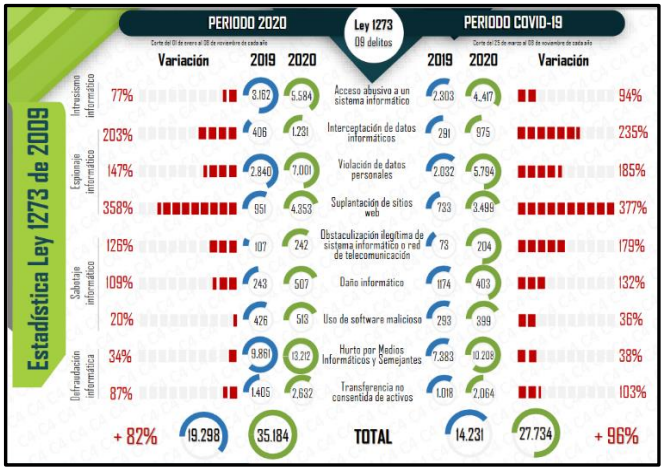


Figura 1. Los 10 principales programas maliciosos que afectan a las instituciones educativas

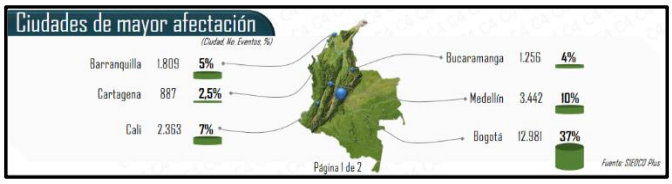
Fuente: (Cybersecurity & Infrastructure Security Agency, 2020)

Las universidades cuentan con un gran número de usuarios que consumen sus recursos todos los días, estudiantes, docentes, administrativos y usuarios externos, por tal motivo es indispensable que cuenten con normas y políticas implementadas para la correcta administración, control y protección de los datos. La universidad ofrece diferentes servicios educativos y de salud a la comunidad, y como tal, debe recopilar, almacenar y administrar todos los datos de sus usuarios, desde notas académicas, información personal, datos financieros, y otros datos aún más sensibles como historias clínicas. La universidad carece de un Sistema de Gestión de Seguridad de la Información (SGSI) lo cual evita un control para el tratamiento de los datos en muchas de sus áreas y permite que sean vulnerables a cualquier ataque cibernético. Según Jeimy Cano, docente de la Universidad del Rosario y experto en seguridad de la información corporativa, Colombia y sus organizaciones, como las entidades educativas, no están preparadas para defenderse ante a una amenaza o ataque cibernético. (Universidad del Rosario, s.f.) Algunos ejemplos que dan evidencia de los ataques que han sufrido las universidades se pueden observar en las noticias cotidianas. El 28 de junio del 2021 la universidad del bosque fue víctima de un ataque cibernético donde se vieron involucrados todos sus sistemas académicos, sistema de gestión de aprendizaje (Moodle), correo electrónico, redes sociales y por su puesto la afectación más grande, la credibilidad ante sus usuarios y su imagen ante el país (El Espectador, 2021). Por otro lado, el 23 de noviembre de 2011 la Universidad Javeriana en sus sedes de Bogotá y Cali también fue víctima de un ataque cibernético que vulneró sus sistemas informáticos y afecto a los estudiantes, profesores y administrativos; este ataque llevó a la universidad a deshabilitar algunos de sus recursos hasta tener plena seguridad de que no se vieran afectados más servicios (Revista

Semana, 2021). Los delitos informáticos y los ciberdelincuentes han aumentado en los últimos años, esto se puede evidenciar gracias a los informes de delitos informáticos y de ciberseguridad que el Centro Cibernético Policial de Colombia ha emitido en conjunto con el C4 (Centro de Comando, Control, Comunicaciones y Cómputo de Bogotá), los cuales son los encargados de articular diferentes herramientas tecnológicas, de operación y recurso humano en la ciudad de Bogotá, con el objetivo de brindar una respuesta coordinada, eficiente y oportuna a eventos de seguridad (CAI Virtual, s.f.). Por medio del SIEDCO (Sistema de Información Estadístico, Delincuencial, Contravencional y Operativo de la Policía Nacional), se observa cómo han aumentado los delitos delincuenciales en la red, y como se utilizan nuevos mecanismos para cometer dichos delitos, estos son más comunes gracias al constante uso del internet y la creación de nuevas tecnologías de la información y comunicaciones (SIEDCO, s.f.). Con la llegada de la pandemia se aceleró el proceso de innovación tecnológica y nuevos retos para las organizaciones incluidas las educativas. El siguiente informe ilustra el aumento de delitos informáticos enfocados en cuatro grandes grupos, Intrusión Informática, Espionaje Informático, Sabotaje Informático y Defraudación Informática, este informe resalta que hay porcentajes de aumento en delitos del más del 100% y algunos alcanzando hasta un 377% como lo es la suplantación de sitios web. Por otro lado, se evidencia que Bogotá tiene un 37% de las afectaciones totales en el país, lo cual indica que es una ciudad objetivo para los ciberdelincuentes.



Estadísticas de ciberdelitos año 2020 en Colombia.
Fuente: (C4 - CENTRO DE COMANDO, CONTROL, COMUNICACIONES Y COMPUTO, 2020)



Porcentajes de afectación de ciberdelitos por ciudades en Colombia
Fuente: (C4 - CENTRO DE COMANDO, CONTROL, COMUNICACIONES Y COMPUTO, 2020)

Dado la justificación del problema tenemos que la relación de los datos de los ciberataques y diferentes modalidades presentados a continuación afectan a los sistemas informáticos de empresas y universidades colombianas, por medio de evidencias en reportes y ejemplos, tenemos que la universidad presenta un alto riesgo de posible afectación si se llegara a perpetuar un incidente informático en su infraestructura tecnológica, dado que, no cuenta al día de hoy con un SGSI (Sistemas de Gestión de Seguridad de la Información), y se ha expresado por parte del equipo de tecnología que no se sigue ningún marco de referencia, ni se tienen bases de conocimiento que puedan apalancar procesos de seguridad, seguridad de la información o ciberseguridad, con los que se pueda responder de manera adecuada a diversos ataques informáticos y que pueda ocasionar grandes inconvenientes para su infraestructura, y la reputación de la universidad.

II. ANALISIS DE ESTRATEGIA ORGANIZACIONAL

Por medio de análisis PEST y DOFA se determina las necesidades de la universidad y su alineación con la estrategia de negocio, por medio de entrevistas y reuniones establecidas en conjunto con la universidad se llevó a cabo la recolección de los datos, en estas reuniones de trabajo se tuvo la oportunidad de participar con las siguientes áreas de la organización, con los respectivos representantes de cada una de ellas:

- Ingenieros de Infraestructura
- Director de Tecnología
- Director Jurídica
- Subdirectora Administrativa
- Directora Financiera
- Director de Comunicaciones
- Directora de Clínicas
- Directora de Recursos Humanos
- Director de Bibliotecas
- Vicerrectora Académica

El análisis se realizó gracias a las definiciones de cada uno de

los puntos de la matriz DOFA, donde se resaltaron las fortalezas de la institución para superar cada una de las debilidades y amenazas. En cada uno de los cuadrantes, se tuvo la oportunidad de discutir con los miembros de la institución a detalle lo incluido en cada uno de ellos, y verificar que estuviéramos abordando en gran medida las falencias o fortalezas que tuviera la institución, gracias a esto, se nos da un estatus lo más cercano a la realidad actual de la universidad, y establecer una línea base para el inicio del diseño.

ANALISIS DOFA

Como resultado del análisis DOFA se identificó que es importante llevar a cabo la implementación del SGSI para la organización y clarificar algunos requerimientos como:

- El servicio de análisis de riesgo es importante con el fin de reconocer riesgos que actualmente no son identificados por el equipo de TICs
- Definir un plan de sensibilización que permita reconocer las principales falencias del público objetivo y enfocar los esfuerzos en mejorar dichos conocimientos.
- La virtualidad y administración de diversos equipos tecnológicos remotamente pueden generar nuevos requerimientos, vulnerabilidades e incidentes que son importantes de responder.
- Es importante correlacionar eventos con distintas fuentes información como, por ejemplo, obtener información de las distintas áreas y el grupo administrativo que las conforman.

ANALISIS PEST

A través de un becnhmark relacionado con las universidades privadas del país se identificaron cuáles eran las normas y el desarrollo económico que representa la universidad y la calidad de la educación que se le pueden brindar a sus estudiantes según su geolocalización, de igual manera se realizaron entrevistas con los siguientes participantes de las áreas:

- Director Jurídica
- Directora Financiera
- Vicerrectora Académica
- Director de Comunicaciones

Como resultado de las reuniones de trabajo, se estableció la comparativa entre el bechmark y el PEST resultante, dándonos una visión panorámica sobre la situación actual de la universidad.

Como resultado del análisis PEST identificamos que es importante llevar a cabo la implementación del SGSI para la institución a través de las siguientes definiciones:

- Los factores socioculturales indican que los planes de entrenamiento deben ser más específicos con el fin de dar el mejor entendimiento de las prácticas de seguridad.
- Dentro de los factores políticos el servicio de análisis de riesgos permitirá dar visibilidad sobre el estado de la empresa y como sus activos son vulnerables.
- El manejo de información personal es una directriz que debe reforzarse debido a las leyes de Colombia y reconocer cual es el impacto en caso de una falla.
- Por último, la modernización y los nuevos requerimientos tecnológicos provocan un gran impacto, por lo tanto, los servicios de configuración y mantenimiento son de vital importancia para mantener buenas prácticas de seguridad.

III. PROPUESTA DE LA SOLUCIÓN

Con relación a la problemática descrita, se ha propuesto como solución realizar el diseño del Sistema de Gestión de Seguridad de la Información en la universidad, el cual tiene como propósito la implementación del SGSI en fases posteriores bajos los siguientes objetivos:

A. Objetivos

Objetivo General:
Diseñar el sistema de gestión de seguridad de la información para la universidad basado en la norma ISO 27003.

Objetivos Específicos:

- Identificar el contexto y propósito de la organización.
- Determinar las necesidades y expectativas de la universidad.
- Determinar el alcance del SGSI.
- Diseñar una política de seguridad de la información en conjunto con la dirección de la institución.
- Analizar riesgos actuales de seguridad referentes al monitoreo de la infraestructura tecnológica y vulnerabilidades de los servidores.
- Definir objetivos y planes de seguridad de la información que la institución debe cumplir.
- Determinar los recursos necesarios para llevar a cabo el SGSI en sus diferentes etapas (establecer, implementar, mantener y mejora continua)

- Implementar un prototipo de la herramienta de monitoreo para la infraestructura tecnológica alojada en el datacenter.

IV. DESARROLLO

ISO27003

La ISO 27003 brinda una orientación sobre los requisitos para un sistema de gestión de seguridad de la información, como se especifica en el ISO 27001, y presenta recomendaciones (debería), posibilidades (puede) y permisos (puede) en relación con ellos.
Se tomó como base la ISO 27003, ya que permite adecuarse a cualquier tipo de organización sin importante que tengan o no implementadas políticas de seguridad de la información.

Ciclo PHVA

En la actualidad, las organizaciones se enfrentan a un nivel tan alto de competencia que para poder crecer y desarrollarse, y a veces incluso para lograr su propia supervivencia, es por esto que han de mejorar continuamente, evolucionar y renovarse de forma fluida y constante. Hemos basados nuestros esfuerzos en que el diseño del SGSI tenga los pilares del ciclo PHVA.
Con la aplicación del PHVA, logramos una eficacia para: reducir costos, optimizar la productividad, ganar cuota de mercado e incrementar la rentabilidad de las organizaciones. Logrando, además, el mantenimiento de todos estos beneficios de una manera continua, progresiva y constante, el cual necesitamos en toda la ejecución e implementación del SGSI.

La ISO 27003 se relaciona con el ciclo PHVA ya que en sus fases se identifica las necesidades de la organización y la valoración de riesgos (Planear) la implementación y operación de procesos (Hacer) hacer seguimiento del desempeño y eficacia (Verificar) practicando la mejora continua del SGSI (Actuar).

V. DISEÑO DEL SGSI

A. Reuniones y Entrevistas

Dentro del proceso de avance del proyecto se generaron diferentes entrevistas con el fin de entender en conjunto con la organización la necesidad particular de la misma.

Las reuniones se realizaron de manera independiente con cada una de las áreas involucradas y a cada uno de los usuarios se le realizaron las mismas preguntas.

- ¿Se ha implementado alguna política de seguridad de la información en la universidad?
- ¿Cómo se lleva a cabo la protección de datos en cada área de la institución?
- ¿El área jurídica a desarrollado o está desarrollando alguna política de seguridad de la información?
- ¿Cuáles son las afectaciones o el impacto que sufren las diferentes áreas en la universidad al no tener políticas definidas de seguridad de la información?
- ¿Existe algún método de capacitación y socialización de las Politicas (en general) dentro de la institución?
- ¿Se ha presentado algún caso relacionado con seguridad de la información como fuga de información, Ciber ataques, Ransomware (secuestro y extorsión), suplantación, entre otros?
- ¿Cuál es la situación actual que más impacta negativamente a la infraestructura tecnológica de la universidad?

B. Alcance del SGSI.

El alcance del sistema de gestión de seguridad de la información está considerado para el área de IT de la universidad, con enfoque en el área de monitoreo de infraestructura tecnológica y escaneo de vulnerabilidades de seguridad, evidenciando los resultados en la mitigación de riesgos por medio del prototipo de implementación.

C. Roles y Responsabilidades

La estructura de gobierno definida para la universidad dentro del marco de diseño del Sistema de Gestión de Seguridad de la Información será la siguiente:

- Junta directiva
- Presidente
- Comité de Riesgos
- Gerencia de Ciberseguridad y Riesgos
- Oficial de Seguridad de la Información
- Colaboradores y terceros

D. Análisis de Riesgos a Través de Magerit

Definición del alcance

El alcance definido para el análisis de riesgos está determinado por los servidores internos de la organización que soportan aplicaciones internas y externas del área de tecnología de la universidad.

Inventario de Activos

Se realiza el levantamiento de información correspondiente al inventario de activos de información de la universidad dando como alcance del proyecto las aplicaciones e infraestructura tecnológica.

Sistema/Aplicación	Confidencialidad	Integridad	Disponibilidad	Criticidad
Firewall	Alta	Alta	Alta	Alto
Switches	Media	Baja	Media	Bajo
Servidor LMS	Baja	Alta	Media	Media
Servidor ERP	Alta	Alta	Alta	Alto
Servidor Académico	Media	Alta	Media	Media
Servidor Biblioteca	Baja	Alta	Baja	Bajo
Servidor Control de acceso	Baja	Baja	Baja	Bajo
Servidor Académico Depresiado	Baja	Baja	Baja	Bajo
Servidor Historias Clinicas	Alta	Alta	Media	Media
Servidor Base de Datos	Alta	Alta	Alta	Alto
Servidor Repositorio institucional	Baja	Alta	Baja	Bajo
Servidor Permanencia estudiantil	Baja	Baja	Baja	Bajo
Servidor de Inventarios	Baja	Baja	Baja	Bajo
Servidor Help Desk	Media	Media	Media	Media
Microsoft 365	Alta	Alta	Alta	Alto
Controlador de Dominio	Alta	Alta	Alta	Alto

Tipo de Información

La institución cuenta con diferente información relacionada con el entorno educativo, administrativo y clínico. En la siguiente tabla se relaciona los tipos de información:

TIPO DE INFORMACIÓN	DESCRIPCIÓN
Confidencial	Historias Clinicas
Confidencial	Datos personales empleados
Confidencial	Bases de datos corporativas
Confidencial	Acceso infraestructura TI
Privada	Notas académicas de grupo estudiantil
Privada	Hoja de vida estudiantes
Privada	Materiales académicos
Pública	Politica de tratamiento de datos
Pública	Estados financieros
Pública	Recursos bibliográficos

Clasificación de Activos

Se ha realizado la clasificación de los activos anteriores basados en los tres pilares de la seguridad de la información:

Confidencialidad	Integridad	Disponibilidad
Información restringida	Alta	Alta
Información Privada	Media	Media
Información Publica	Baja	Baja
Información No Publica	No Clasificada	No Clasificada

(MINTIC, 2016)

Criticidad de los activos

Mediante la tabla de criticidades, fue posible determinar la importancia de cada activo de información dentro de la organización.

CRITICIDAD	
ALTA = 3	Aquellos activos en los cuales la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) se clasifica como alta.
MEDIA = 2	Aquellos activos de información para los que la información resulta alta en al menos una propiedad o por lo menos una de estas es clasificada como nivel medio.
BAJA = 1	Son los activos de información en los que su clasificación de información en cualquiera de los niveles se considera como baja.

(MINTIC, 2016)

Degradación del valor

Se valida cada uno de los activos y se determina bajo la siguiente escala el perjuicio del activo en caso de materialización de una amenaza:

Escala degradación del valor	Valor
Muy alta	5
Alta	4
Media	3
Baja	2
Muy baja	1

Valoración de probabilidad de ocurrencia

Se valida cada uno de los activos y se determina bajo la siguiente escala la probabilidad de materialización de una amenaza:

Escala probabilidad de ocurrencia	Valor
Muy frecuente	5
Frecuente	4
Normal	3
Poco frecuente	2
Muy poco frecuente	1

Análisis de vulnerabilidades

Se realizó la instalación de la herramienta Nessus (Versión trial) la cual nos ofrece una visión acerca de las vulnerabilidades que actualmente presenta la universidad dentro de su infraestructura, encontrando:

- Descubrimiento de sistemas operativos y versiones de los mismos
- Vulnerabilidades en los servidores internos de la universidad, con riesgo alto y crítico.
- Evidencia de distintos tipos de vulnerabilidades

- Análisis de aplicaciones web internas y servidores de servicios críticos para la organización

Dado lo anterior, dentro de las reuniones de seguimiento con la universidad, se da un estado parcial de las vulnerabilidades actuales de la infraestructura, que sirve como insumo inicial para remediación con el siguiente enfoque:

- Solución de vulnerabilidades Criticas y Altas, y tratamiento de medias y bajas para evitar que se conviertan en críticas por no gestión.

Análisis de amenazas

De origen natural:

- Incendios en instalaciones de datacenter.
- Condiciones climáticas anómalas
- Inundaciones que puedan dañar instalaciones de corriente
- Desastres Naturales

Del entorno:

- Contaminación, polvo excesivo, corrosión de metales
- Corte de la fuente de alimentación de energía al datacenter de servidores
- Corte de las redes de comunicación en el datacenter de servidores
- Suspensión del suministro de red
- Interrupción de los proveedores de servicios
- Terrorismo
- Eliminación, destrozo de dispositivos o soportes de almacenamiento
- Pandemia COVID-19

Defectos de las aplicaciones:

- Contar con infraestructura obsoleta para realizar escaneos de vulnerabilidades a la infraestructura
- No disponer de software especializado para el escaneo de vulnerabilidades y monitoreo de la infraestructura
- Existencia de vulnerabilidades en los sistemas o servidores
- Errores del software de la organización
- Fallo de dispositivos o sistemas
- Mal funcionamiento de dispositivos o sistemas
- Falta de recursos (Memoria RAM, DD, etc) informáticos para el buen funcionamiento de los sistemas
- Ataques de denegación de servicio
- Software malicioso
- Tener licencias de antivirus vencidas

Causadas por las personas de forma accidental

- Falta de conocimiento o profundización en los procesos internos de la compañía para el diseño del SGSI
- Desconocimiento por parte de los empleados de los pilares de seguridad de la información
- Ausencia de pruebas de vulnerabilidades a la infraestructura
- Información o productos de una fuente no confiable
- Uso incorrecto o administración de dispositivos y sistemas
- Violación de leyes o regulaciones por desconocimiento
- Ausencia de personal calificado para la administración de los sistemas
- Ataques de Ingeniería Social a los funcionarios y estudiantes de la universidad

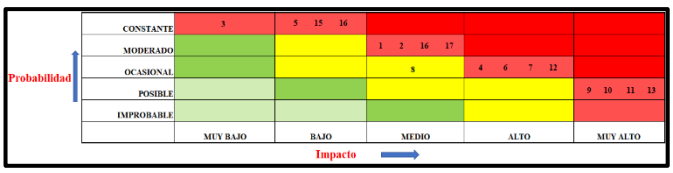
Causadas por las personas de forma deliberada

- Deseo o intensión maliciosa por parte de un empleado de causar afectación a la organización
- Inadecuada segregación de funciones
- Espionaje y escucha de información confidencial.
- Coerción, extorsión o corrupción.

Valoración del Riesgo

Escala de riesgo		
4 A 5	CONSTANTE	MUY ALTO IMPACTO
3 A 4	MODERADO	ALTO IMPACTO
2 A 3	OCASIONAL	MEDIO IMPACTO
1 A 2	POSIBLE	BAJO IMPACTO
0 A 1	IMPROBABLES	MUY BAJO IMPACTO

Escala de Riesgo

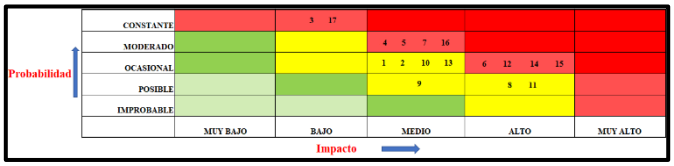


Mapa de valoración del Riesgo

Podemos observar que la mayor cantidad de activos se encuentra en riesgo de un nivel moderado de probabilidad de materialización de amenazas, sin embargo, muy cercano a tener un alto impacto para la organización si estos no son tratados, los cuales fueron informados a la organización para ser tratados con prioridad.

Valoración del riesgo residual

La siguiente imagen muestra la categorización de los activos después de haber realizado la mitigación de vulnerabilidades de algunos de los servidores, producto del escaneo realizado y entregado a la organización para su tratamiento prioritario.



Mapa de valoración del Riesgo Residual

E. Ejemplo Análisis de Riesgo

Activo = Controlador de dominio

Activo	Criticidad	Degradación de Valor	Impacto
Controlador de dominio	Alta = 3	Muy alta = 5	4,2

Amenazas

Amenaza	Probabilidad de Ocurrencia
Desastres naturales	Poco frecuente = 2
Corte en redes de comunicación	Frecuente = 4
Terrorismo	Normal = 3
Vulnerabilidad en el sistema	Frecuente = 4
Fallo del dispositivo	Normal = 3
Falta de resurosos (RAM, Disco, CPU)	Normal = 3
Malware	Frecuente = 4
Insiders	Poco frecuente = 2
	Tota = 3,125

Riesgo

Activo	Impacto	Probabilidad de ocurrencia	Riesgo	Categorización
Controlador de dominio	4,2	3,125	3,6625	

F. Riesgos

El siguiente listado de riesgos fue obtenido después de realizar el análisis en conjunto con el personal de la universidad y observando cada una de las falencias encontradas dentro de los procesos anteriores.

Riesgos Generales de TI:

- Perdida de información a causa de una amenaza natural.
- Indisponibilidad de los servicios debido incendios en las instalaciones de datacenter
- Robo de información sensible
- Riesgo reputacional
- Riesgo normativo

Riesgos Asociados al SGSI

- Vulneración de los sistemas
- Fuga de información por ataques a los sistemas informáticos de la organización
- Indisponibilidad de los servicios debido a saturación de recursos generados por ataques de DDoS
- Manipulación de la información contenida en las BD debido a ataques cibernéticos afectando la integridad de la información.
- Secuestro de información debido a ataques de ransomware
- Insuficiencias operativas de software
- SGSI ineficaz
- Divulgación de información sensible
- Fuga de información por acceso sin restricción a los servidores por parte de los empleados de la compañía
- Suplantación de identidad de los administradores de los sistemas
- Manipulación de la data por parte de funcionarios internos afectando la confidencialidad e integridad de la información
- Manipulación malintencionado hardware y software
- Robo de dispositivos, soportes de almacenamiento y documentos
- Pérdida de dispositivos, soportes de almacenamiento y documentos
- Manipulación malintencionada de información
- Intrusión por parte de un atacante en los sistemas de la organización
- Manipulación accidental de servidores por parte del personal interno administrador

Riesgos del Proyecto

- Planificación del diseño del SGSI desenfocado de los objetivos estratégicos de la organización
- SGSI ineficaz
- Riesgo normativo
- Implantar erróneamente un SGSI puede llegar a afectar planes estratégicos de la organización, afectando la consecución de objetivos establecidos, toma de decisiones y a la posición competitiva en el mercado de la organización.
- Definición errónea del equipo de trabajo - Aumento de los costes del proyecto
- Retrasos de proyecto.
- Adaptación e integración inadecuada del SGSI en las actividades habituales por parte de los colaboradores de la organización

G. Políticas de Seguridad de la Información

Se ha generado la política de seguridad de la información y políticas específicas como referentes en la norma ISO 27001, Las cuales nos ayudarán en el proceso de implementación del SGSI y en la adhesión exitosa de las buenas prácticas:

- Política general de seguridad de la información.
- Política de gestión de activos de información.
- Política de desarrollo seguro de software.
- Política de gestión de incidentes.
- Política de gestión de vulnerabilidades.

H. Plan de Comunicación y Divulgación del SGSI

El objetivo principal del plan de comunicación es crear una estructura para la correcta divulgación y toma de conciencia sobre el SGSI en la universidad en el cual se encuentran actividades de capacitación, divulgación de políticas, sensibilización y definición de responsabilidad referentes a la seguridad de la información en la universidad incluyendo sus colaboradores, estudiantes, docentes y usuarios externos que tengan contacto con la institución.

La comunidad en la universidad debe tomar conciencia de que existen políticas relacionadas con seguridad de la información y deben saber dónde se encuentra dicha información. No es necesario que toda la comunidad conozca de manera detalla las políticas, pero si debe conocer, comprender, aceptar e implementar los objetivos y requisitos que se deriven de ellas.

Canales de comunicación

Los canales de comunicación se han establecido para comunicar y distribuir información desde el grupo de comunicaciones se describen a continuación:

Canales de comunicación para las áreas internas de la organización:

- Correo electrónico para difundir información a la organización o contactar al equipo de seguridad.

- Página web donde se podrán observar las políticas de seguridad de la información que se entregan al público exterior.
- Intranet en la cual se podrá encontrar:
    - Formularios Web para incidentes relacionados con seguridad de la información
    - Puntos de contacto como email y teléfono de diferentes áreas
    - Consulta de material informativo
- Teléfono disponible para contactar a las diferentes áreas que están involucradas en el SGSI de la institución (Modalidad On-Call)
- Sistema interno de mensajería (chat) - Este medio se utilizará para responder preguntas, prestar soporte interno o consultar el estado de un incidente previamente, pero no podrá ser utilizado para recopilar evidencia.
- Sesiones síncronas virtuales que permiten la capacitación del personal de manera remota
- Sesiones presenciales en aulas o auditorios para exponer, clarificar, capacitar y retroalimentar los procesos y políticas del SGSI en la universidad.
    - Videos de capacitación con material informativo

Canales de comunicación para Estudiantes y Profesores:

- Correo electrónico para difundir información sobre campañas de sensibilización y alertas.
- Página web donde se podrán observar las políticas de seguridad de la información que se entregan al público exterior.
- Sesiones presenciales en aulas o auditorios para exponer, clarificar, capacitar y retroalimentar los procesos y políticas del SGSI en la universidad.
- Formularios para reportar vulnerabilidades o reportar el mal uso de los recursos tecnológicos (con la opción de anonimato)
- Videos de capacitación con material informativo

Los formularios Web para el reporte de incidentes serán el principal medio de recopilación de evidencia, la cual debe tener certificados TLS y almacenarse de manera encriptada. Cualquier otra evidencia que necesite recopilarse deberá entregarse cifrada al equipo de Seguridad mediante correo electrónico únicamente.

Canales de comunicación para personal externo la organización:

- Correo electrónico para difundir información de la organización y difundir información sobre campañas de sensibilización y alertas.

- Página web donde se podrán observar las políticas de seguridad de la información que se entregan al público exterior.

Programa de mensajería para usuarios internos y externos

A través del grupo de comunicaciones de la institución se crearán mensajes relacionados con las políticas de seguridad de la información que la universidad implementará y que posteriormente se divulgaran a través de los canales de comunicación.

Creación de material informativo y capacitación

Dentro del plan de comunicación, el área de comunicaciones se encargará de crear material informativo y de capacitación el cual será integrado a toda la comunidad de la institución.

Para el desarrollo de esta fase, el área de comunicaciones tendrá reuniones periódicas con las demás áreas de la institución involucradas en la implementación del SGSI como lo son la dirección Administrativa, la dirección Académica, Dirección Financiera, TI, entre otras.

Evaluación de conocimientos en capacitaciones

Después de finalizar los procesos de capacitación con la comunidad de la universidad, se procederá con un proceso de verificación de conocimiento y comprensión de los temas enseñados a través de una evaluación aleatoria la cual podrá ser escrita u oral.

Auditoria y retroalimentación constante

Es indispensable auditar y validar que el personal administrativo, grupo docente y estudiantil de la universidad, si estén actuando conforme a las políticas y capacitaciones brindadas. Para esto, con el apoyo del área de TI, se estará auditando todos los procesos para velar el correcto cumplimiento de las políticas y en caso de presentarse comportamientos erróneos o anómalos se procederá con un proceso de retroalimentación al usuario y al área involucrada.

El proceso de retroalimentación consistirá en una etapa de capacitación y evaluación como se menciona en los numerales anteriores.

VI. PROTOTIPO DE LA IMPLEMENTACIÓN

Con el fin de obtener un entregable de valor para la universidad, dentro del diseño del SGSI y más específicamente acotándolo a las etapas del Ciclo PHVA, llegamos a la etapa del Hacer, dado que en esta fase se implementa la selección de controles adecuados para medir los riesgos, y nosotros hemos determinado el monitoreo como uno de esos pilares de control para la organización, con esta fase iniciamos la de implementación del SGSI.

Dentro del roadmap herramental propuesto para robustecer la seguridad de la universidad, basamos los esfuerzos en tres principales:

- Como piloto principal desarrollado dentro de la universidad se llevó a cabo el despliegue e implementación de la herramienta de monitoreo de infraestructura de servidores.

- Como herramientas complementarias para llevar acabo el análisis de riesgos y revisar principales vulnerabilidades se llevó a cabo el despliegue e implementación de una versión gratuita de Nessus Tenable de escaneo de vulnerabilidades de infraestructura.

- Con respecto al roadmap propuesto, continuamos con el despliegue de la solución Elastic Security SIEM y analítica de seguridad, la cual complementará las dos anteriores, teniendo la capacidad de correlacionar los eventos y dando la oportunidad de visualizar comportamientos anómalos para detección de posibles incidentes de seguridad.

Con la implementación de la herramienta de monitoreo, se considerará el mejoramiento sustancial de las problemáticas

evidenciadas en las entrevistas las cuales se llevaron a cabo dentro de las primeras etapas consideradas etapas de diseño y planificación del SGSI, dándonos una visual actual de la universidad en cuanto a seguridad, donde cada uno de los representantes de las áreas invitadas lograron dar un contexto general actual tanto de sus fortalezas como de sus amenazas, dado lo anterior, con la implementación del monitoreo de infraestructura de TI, se tendrá la posibilidad de tener un control de sus servidores de manera organizada, con enfoque al crecimiento de los mismos, por consiguiente se ha realizado la entrega del prototipo de implementación a la universidad con las siguientes características y generalidades de la herramienta:

Software de monitoreo de red – Manage Engine OpManager,

Las empresas confían en las redes para todas las operaciones. Por lo tanto, el monitoreo de la red es crucial para cualquier negocio. Hoy en día, las redes se extienden por todo el mundo y se han establecido múltiples enlaces entre centros de datos separados geográficamente, nubes públicas y privadas. Esto crea múltiples desafíos en la gestión de la red. Los administradores de red deben ser más proactivos y ágiles en el monitoreo del rendimiento de la red. Sin embargo, esto es más fácil decirlo que hacerlo.

ManageEngine OpManager, es una solución de monitoreo de red asequible y fácil de usar. Monitorea dispositivos de red como routers, switches, firewalls, balanceadores de carga, controladores de LAN inalámbrica, servidores, máquinas virtuales, impresoras, dispositivos de almacenamiento y todo lo que tiene una IP y está conectado a la red. OpManager monitorea continuamente la red y proporciona una visibilidad profunda y control sobre ella. En caso de una falla, puede detectar fácilmente la causa raíz y eliminarla antes de que las operaciones se vean afectadas.

Beneficios de implementación de la solución

- Monitoreo de redes en tiempo real
- Monitoreo de servidores físicos y virtuales
- Umbrales Multi-nivel

VII. TRABAJO FUTURO

Cuando nos referimos a los pasos siguientes dentro del proyecto, debemos revisar básicamente el trabajo desarrollado hasta el día de hoy, la construcción del diseño del SGSI para la organización nos dio el punto de partida específico para tener unas bases sólidas sobre las cuales consolidar la implementación, posteriormente las consolidación y mejora del mismo, es así como veremos en próximos meses y años la implementación del mismo con las siguientes etapas a considerar:

- Planificación
- Implementación del Sistema de Gestión de Seguridad de la Información
- Fase de control o de verificación
- Actuación, mantenimiento y mejora

En cada una de estas y de acuerdo al cronograma de actividades se llevarán a cabo las actividades por cada uno de los responsables definidos dentro del diseño, con sus respectivos roles y responsabilidades.

Dentro de este plan tenemos:

- Requerimientos y compromisos del SGSI
- Cronograma de actividades de planeación y diseño:
    - Planificación del SGSI
    - Equipo con roles y responsabilidades
    - Políticas de seguridad de la información
    - Roadmap Herramental
    - Preparación para la ejecución del SGSI.
    - Plan de comunicación del SGSI.
    - Presupuesto del proyecto

VIII. REFERENCIAS

[1] C4 - CENTRO DE COMANDO, CONTROL, COMUNICACIONES Y COMPUTO. (2020). CAI VIRTUAL POLICIA NACIONAL DE COLOMBIA. Obtenido de CENTRO CIBERNETICO POLICIAL: https://caivirtual.policia.gov.co/sites/default/files/balance_ciberrcrimen_2020_-_semana_45.pdf

[2] CAI Virtual. (s.f.). CAI Virtual. Obtenido de https://caivirtual.policia.gov.co/sites/default/files/balance_ciberrcrimen_2020_-_semana_45.pdf

[3] Cybersecurity & Infrastructure Security Agency. (10 de diciembre de 2020). cisa. Obtenido de https://www.cisa.gov/uscert/ncas/alerts/aa20-345a

[4] Edita: © Ministerio de Hacienda y Administraciones Públicas - NIPO: 630-12-171-8. (10 de 2012). administracionelectronica.gob.e. Obtenido de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

[5] El Espectador. (28 de Junio de 2021). El Espectador. Obtenido de https://www.elespectador.com/educacion/la-universidad-el-bosque-fue-victima-de-un-ciberataque/

[6] Elastic. (2022). www.elastic.co. Obtenido de https://www.elastic.co/es/pdf/guide-to-high-volume-data-sources-for-siem

[7] Fernández, Á. P. (16 de 11 de 2019). jlglobalservices.com.co. Obtenido de https://www.jlglobalservices.com.co/web/ciclo-phva/

[8] funcionpublica.gov.co. (s.f.). Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

[9] funcionpublica.gov.co. (s.f.). Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488#:~:text=HABEAS%20DATA&text=Dicta%20las%20disposiciones%20generales%20del,la%20proveniente%20de%20terceros%20pa%C3%ADses.

[10] https://ciberseguridad.blog/. (13 de 11 de 2022). CIBERSEGURIDAD.BLOG. Obtenido de https://ciberseguridad.blog/iso-27001-2022-controles-nuevos-en-el-estandar-de-ciberseguridad-por-excelencia

[11] IC3. (2021). IC3. Retrieved from https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

[12] ICONTEC. (2018). *GTC-ISO/IEC 27003.* Bogotá, D.C.

[13] *isotools.org*. (s.f.). Obtenido de https://www.isotools.org/2015/02/20/en-que-consiste-el-ciclo-phva-de-mejora-continua

[14] MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. (10 de 2012). Madrid, España.

[15] *ManageEngine.* (2022). Obtenido de https://www.manageengine.com/latam/network-monitoring/

[16] ManageEngine. (2022). *ManageEngine*. Obtenido de https://www.manageengine.com/latam/network-monitoring/

[17] manageengine.com. (s.f.). *manageengine.com*. Obtenido de https://www.manageengine.com/es/network-monitoring/

[18] Ministerio de Cultura del Perú. (19 de 11 de 2020). ROLES Y RESPONSABILIDADES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – SGSI. Perú.

[19] MINTIC. (15 de Marzo de 2016). *www.mintic.gov.co*. Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

[20] *Normaiso27001*. (s.f.). Obtenido de https://normaiso27001.es/fase-4-planificacion-del-sgsi/

[21] *nqa.com*. (s.f.). Obtenido de https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

[22] *pmg-ssi.com*. (06 de 08 de 2014). Obtenido de https://www.pmg-ssi.com/2014/08/iso-2700-12013-politica-roles-responsabilidades-autoridades-organizacion

[23] Revista Semana. (23 de Noviembre de 2021). *Revista Semana*. Obtenido de https://www.semana.com/nacion/articulo/la-universidad-javeriana-confirma-que-sufrio-ataque-informatico-en-bogota-y-cali/202153/

[24] *secretariasenado.gov.co*. (s.f.). Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_1341_2009.html

[25] SIEDCO. (s.f.). *Secretaria de Seguridad, Convivencia y Justicia*. Obtenido de https://scj.gov.co/es/oficina-oaiee/bi/seguridad_convivencia/siedco

[26] Tenable. (s.f.). *https://es-la.tenable.com/*. Obtenido de https://es-la.tenable.com/solutions/vulnerability-management

[27] UNICOC. (s.f.). *Unicoc*. Obtenido de https://unicoc.edu.co

[28] Universidad de Cundinamarca. (23 de 02 de 2021). MANUAL DE ROLES Y RESPONSABILIDADES EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. FUSAGASUGA, CUNDINAMARCA, COLOMBIA.

[29] Universidad del Rosario. (s.f.). *urosario*. Obtenido de https://www.urosario.edu.co/UCD/Colombia-no-esta-preparada-ante-un-ciberataque/