Planificación y Desarrollo de la Fase 2 del Esquema Gubernamental de Seguridad de la Información de la Universidad de las Fuerzas Armadas "ESPE"

Departamento de Ciencias de la Computación

Carrera de Tecnologías de la Información

Canchigña Llumiquinga, Esteban Andrés

Parra Martínez, Christian Fabricio

CONTENIDO

Introducción

- Antecedentes
- Justificación
- Objetivos

Marco Teórico

- Seguridad de la información
- Sistema de gestión de la seguridad de la información SGSI
- Metodologías de análisis de riesgo
- Esquema Gubernamental de seguridad de la información EGSI

Planificación del SGSI

Diseño del SGSI

Conclusiones y recomendaciones

INTRODUCCIÓN

ANTECEDENTES Y PROBLEMA

- El empleo de equipos informáticos de forma no controlada representa una brecha importante en el campo de la seguridad informática.
- La Unidad de Seguridad Integral de la ESPE a fin de brindar la protección a la información implementa el Esquema Gubernamental de Seguridad de la Información (E.G.S.I.).
- Actualización a la versión 2 del E.G.S.I en base a la norma ISO 27001.

JUSTIFICACIÓN

- Planificación e implementación de un (SGSI), permitirá aplicar los controles adecuados en base a la confidencialidad, disponibilidad e integridad de la información.

- Análisis y Definición del Tratamiento de Riesgos de la Fase 2 de la Implantación del EGSI.

EGSI ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN

OBJETIVO GENERAL

Realizar la Planificación y Desarrollo de la Versión 2 del EGSI de la Universidad de las Fuerzas Armadas ESPE, en base de las normas ISO 27001, ISO 27002, ISO 27003, ISO 27005, ISO 31000, para cumplir los requerimientos establecidos en el acuerdo 2019-025-MINTEL y estar preparados para una auditoría de precertificación.

OBJETIVOS ESPECÍFICOS

- Establecer el estado del Arte
- Realizar la planificación de la versión 2 del EGSI de la ESPE.
- Realizar el análisis y valoración de riesgo.

OBJETIVOS ESPECÍFICOS

- Tratamiento de riesgos y definición de salvaguardas.
- Plan de implantación de salvaguardas.

MARCO TEÓRICO

SEGURIDAD DE LA INFORMACIÓN

- Se considera un factor clave para el éxito de las organizaciones y empresas.
- Confidencialidad, integridad y disponibilidad.
- Vulnerabilidad ante riesgos que reduce la competitividad y rentabilidad.
- Ciberseguridad como conjunto de acciones para la protección de la información.

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

- Un SGSI define las políticas, desarrollo y herramientas con el propósito de garantizar la seguridad en organizaciones, dicho proceso incluye la introducción de procedimientos específicos.

METODOLOGÍA DE ANÁLISIS DE RIESGO

ISO IEC-27000

- ISO 27001 establecer, implementar y mantener el mejoramiento del SGSI.
- Planificación.
- Operación.
- Evaluación.

METODOLOGÍA DE ANÁLISIS DE RIESGO

ISO IEC-27000

- ISO 27002 determina principios para la seguridad.
- Aplica buenas prácticas de gestión considerando un conjunto de controles y los riesgos existentes.
- Políticas de seguridad.
- Organización de la seguridad.
- Seguridad en RRHH.
- Gestión de activos.
- Control de acceso.
- Gestión de incidentes y continuidad del negocio.

METODOLOGÍA DE ANÁLISIS DE RIESGO

ISO IEC-27000

- ISO 27003 guía para diseñar e implementar un SGSI, especificaciones necesarias.
- Aprobación de la dirección.
- Descripción de políticas y alcance.
- Análisis organizacional.
- Evaluación para valoración del riesgo y el respectivo tratamiento.
- Diseño del SGSI.

METODOLOGÍA DE ANÁLISIS DE RIESGO

ISO IEC-27000

- ISO 27005 principios para la gestión de riesgos.
- Importancia de los activos de información.
- Aspectos legales.
- Cumplimiento en las operaciones preservando la seguridad.
- Perspectivas de cada parte de la organización.
- Identificación de repercusiones.

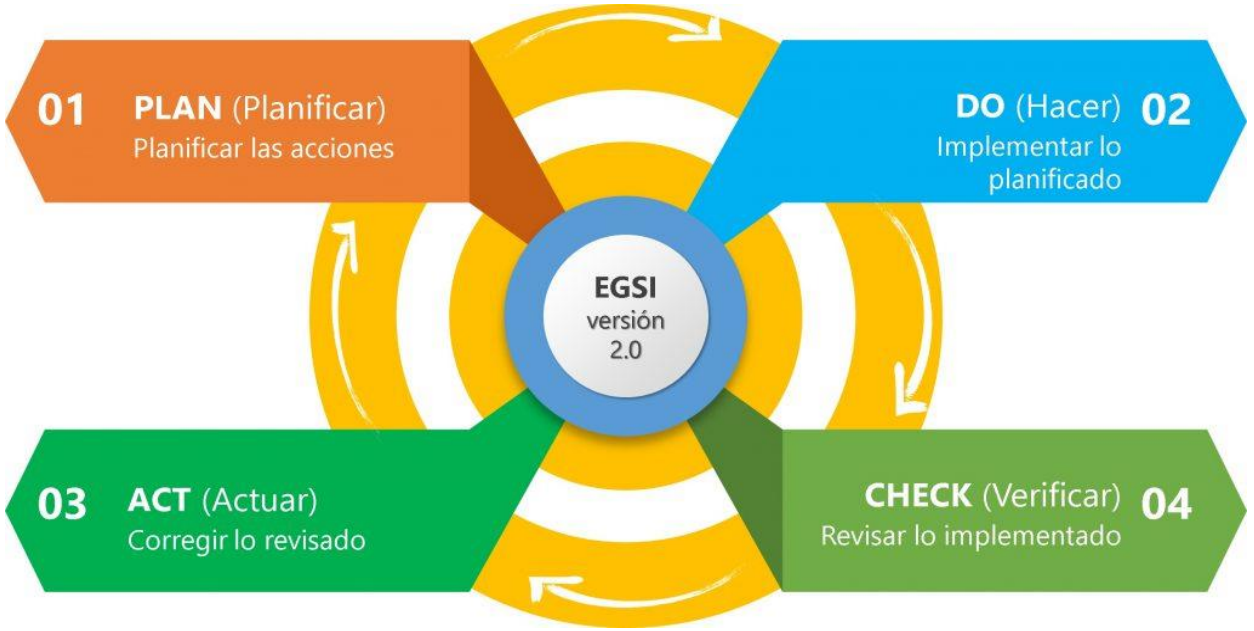
METODOLOGÍA DE ANÁLISIS DE RIESGO

ISO IEC-27000

- ISO 31000 norma que proporciona principios y directrices sobre gestión de riesgos.
- Creación y protección del activo.
- Integración de procedimientos.
- Determinar decisiones.
- Identificación perspectiva sistemática.
- Soporte de información relevante.
- Transparencia e inclusión de puntos de vista.
- Garantizar la continuidad de la organización.

ESQUEMA GUBERNAMENTAL DE LA SEGURIDAD DE LA INFORMACIÓN

- Publicación mediante Acuerdo Ministerial No. 025-2019 en el Registro Oficial.
- Implementación obligatoria para instituciones de la Administración Pública Central.

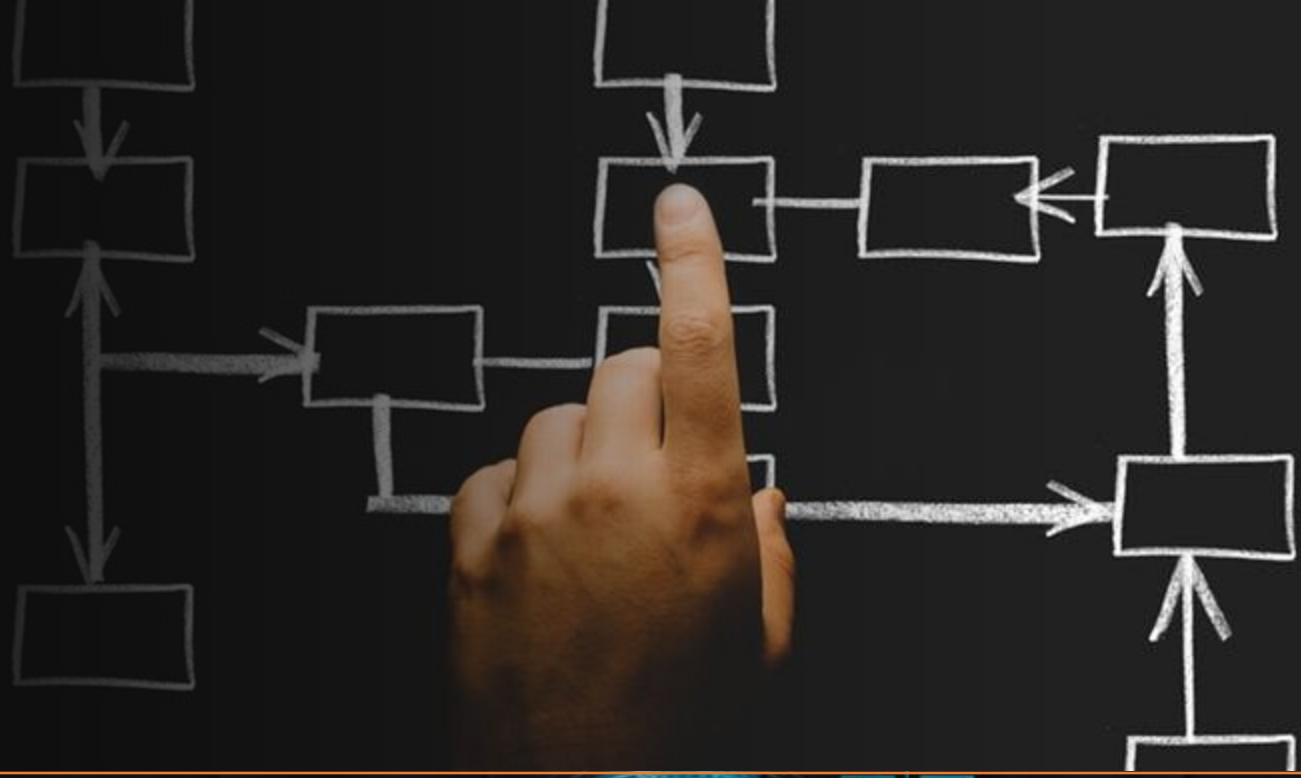


PLANIFICACIÓN SGSI

INTRODUCCIÓN Y DESCRIPCIÓN DEL PROYECTO

- Etapas para describir el proyecto, establecer límites, políticas y alcance del proyecto donde se identificará los límites físicos, organizacionales y de TI.
- Evaluar y determinar los controles adecuados.
- Creación del caso de negocio con prioridades, objetivos y estructura de la organización.

ALCANCE



Macroprocesos ESPE

Macroprocesos	Descripción
Macroprocesos de dirección o gobierno.	Están orientados hacia el cumplimiento de la misión y la materialización de la visión institucional de la ESPE, son responsables de establecer políticas, planes estratégicos, resoluciones y regulaciones contribuyendo al sistema de educación superior.
Macroprocesos habilitantes de asesoría.	Encargados de generar productos secundarios de asistencia técnica especializada y de asesoría.
Macroprocesos habilitantes de apoyo.	Tienen la responsabilidad de generar los productos secundarios que materializan los recursos humanos, materiales, financieros, tecnológicos y documentales.
Macroprocesos agregadores de valor.	Responsables de generar el portafolio de productos primarios que responden a la misión y al modelo de gestión de la ESPE.

MARCO LEGAL

- Ley de Comercio Electrónico, Firmas y Mensajes de Datos
- Ley Orgánica de Educación Superior LOES – CES
- Ley Orgánica de Protección de Datos personales

ALCANCE SGSI

- Matriz de priorización de los Macroprocesos de gestión

MACROPROCESOS	Dirección	Asesoría	Apoyo	Agre. de Valor	Total	Orden
Dirección		0,5	0,5	0,5	1,5	2°
Asesoría	0,5		0,5	0	1	3°
Apoyo	0,5	0,5		0	1	4°
Agre. de Valor	0,5	1	1		2,5	1°

Criterios de Puntuación	
Es más importante	1
Es igual de importante	0,5
Es menos importante	0

ALCANCE SGSI

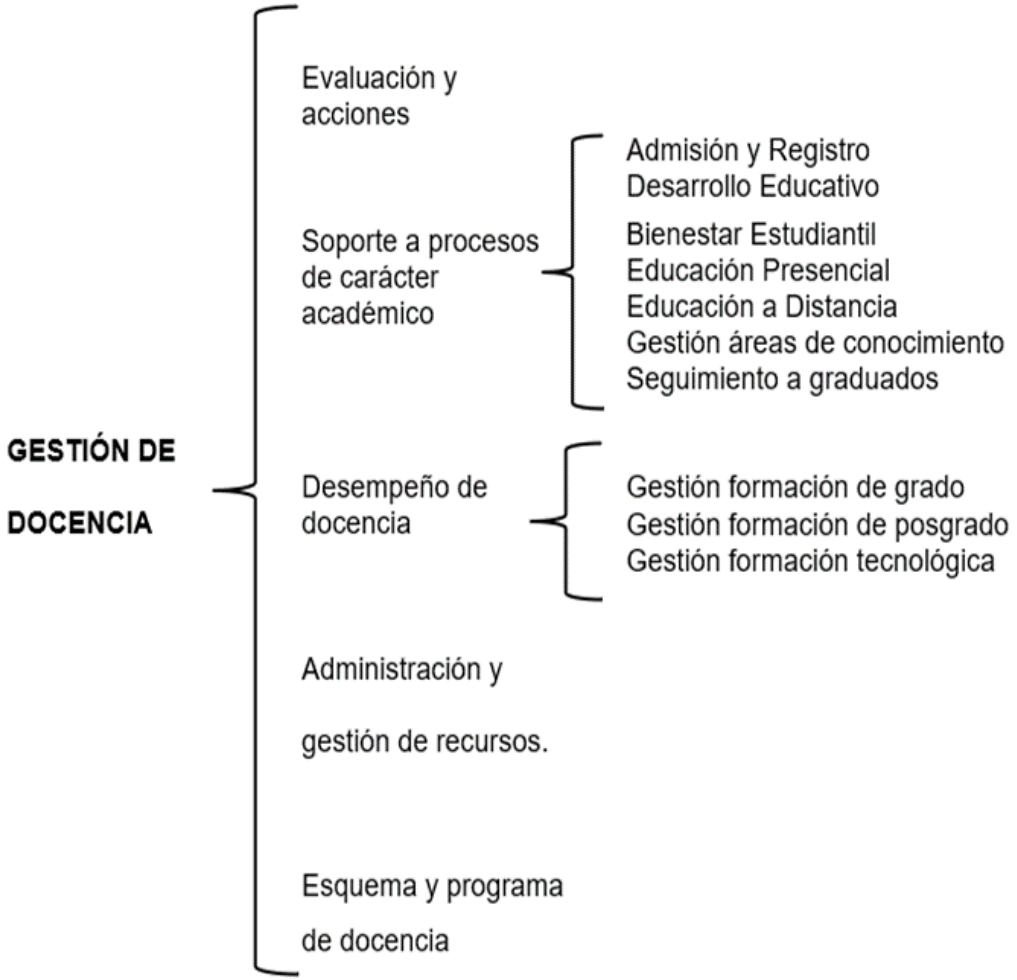
- **Resultado Matriz de Holmes**

La consideración del proceso de Gestión de Docencia como crítico y de mayor importancia ha podido ser identificado gracias a la priorización en la Matriz de Holmes y sin su correcto funcionamiento, no se cumplen los objetivos institucionales.

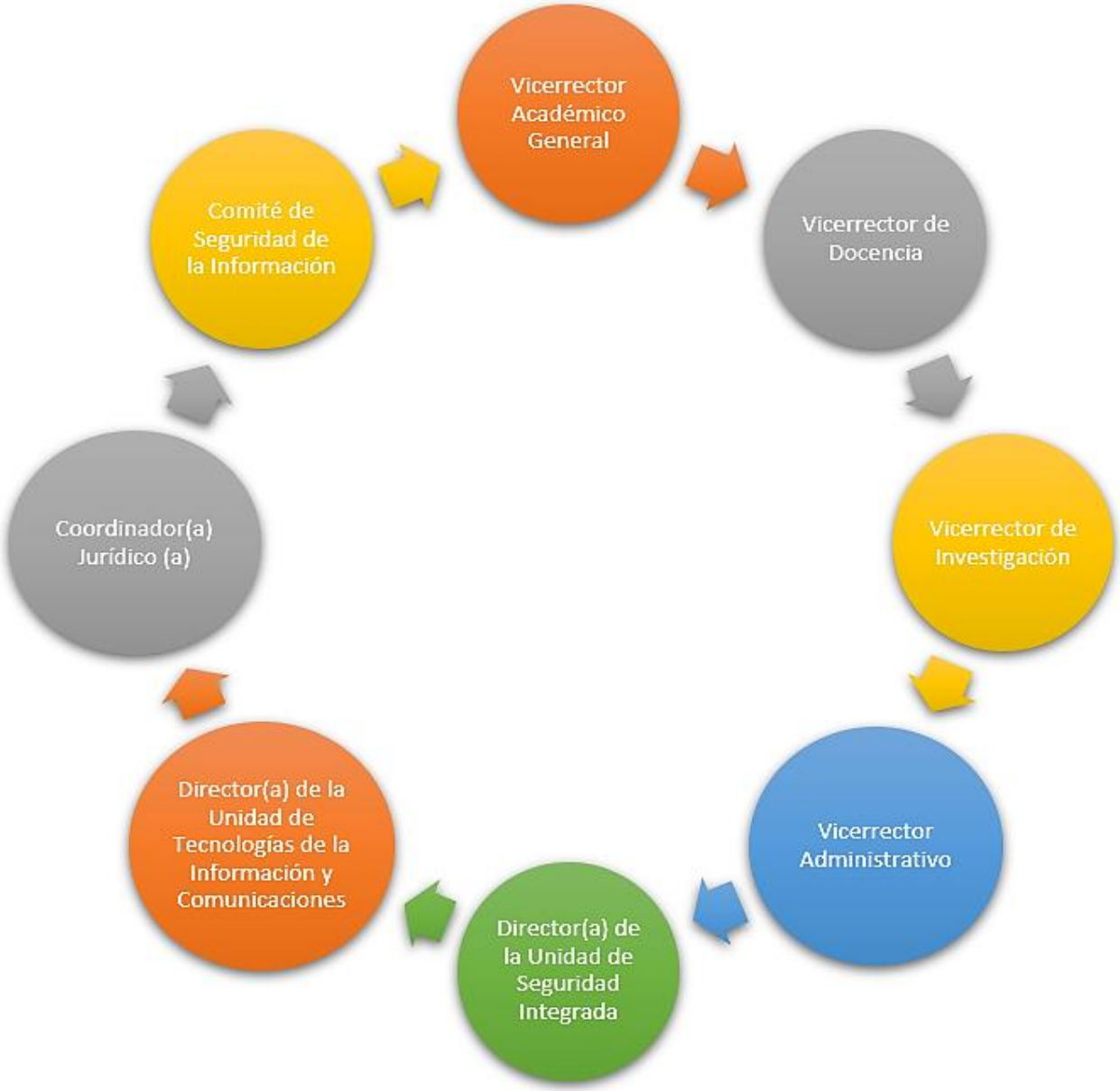
Prioridad	Procesos	Total
4	Vinculación con la sociedad	0
3	Investigación	1
2	Coordinación académica general	2
1	Docencia	3

LÍMITES ORGANIZACIONALES

Procesos relacionados con Gestión de Docencia en la Universidad de las Fuerzas Armadas ESPE



Roles y Funciones Directivos



LÍMITES TIC

Proceso	Activo	Tipo de Activo
Admisión y Registro	Servidor Virtual principal para matriculas de estudiantes	Aplicación
	Servidor virtual redundante para matriculas de estudiantes	Aplicación
	Servidor virtual para el servicio de inscripción de estudiantes	Aplicación
	Servidor virtual principal para el módulo de Workflow	Aplicación
	Servidor virtual para el módulo de registros de pagos en línea	Aplicación
	Servidor incluido para Banner	Servidor Hardware
	Sistema operativo funcional en ESPEMATICO	Software

LÍMITES FÍSICOS

SEDES

SITIO	UBICACIÓN
Matriz	Provincia: Pichincha Cantón: Rumiñahui Dirección: Av. General Rumiñahui s/n y Ambato
	Unidades Académicas Externas
IASA I	Provincia: Pichincha Cantón: Rumiñahui Dirección: Barrio San Fernando – Hacienda el Prado
Instituto de Idiomas	Provincia: Pichincha Cantón: Rumiñahui Dirección: Av. 6 de Diciembre y Río Coca

Identificación de los activos del SGSI

Activos de información

Banner	BDD Baner	BDD Educativa	BBD MySQL Micrositios Educativa	Eduroam
ERP	Espemático	Monitoreo y Seguridad	Pentaho	Quipux
Servidor Lab DECC	Red ESPE	Prácticas Preprofesionales	Open Journal Pruebas	Formularios
Open Journal	Workflow			

ANÁLISIS DE RIESGO

VULNERABILIDAD

- Una vulnerabilidad representa una debilidad existente en un sistema que puede ser utilizada por una persona malintencionada para comprometer su seguridad.
- ISO 27005 Anexo D (Vulnerabilidades y métodos para la valoración de la vulnerabilidad)

AMENAZA

- Una amenaza representa un factor que aprovecha una vulnerabilidad con la finalidad de atacar un sistema informático y obtener un beneficio y dañar servicios importantes.

- ISO 27005 Anexo C (Ejemplos de amenazas comunes).

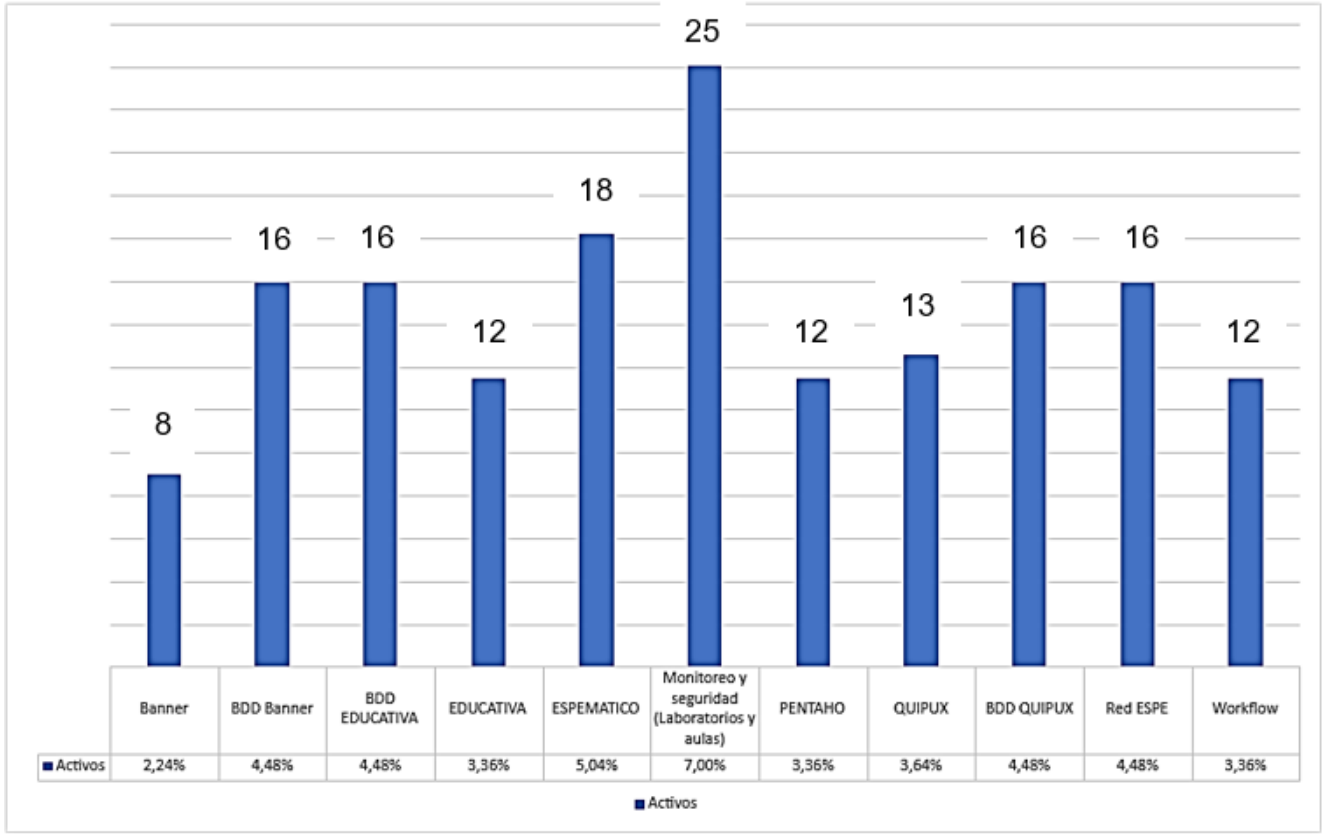
RIESGO

NIVEL DE RIESGO

NIVELES DE RIESGO		
Nivel	**Intervalo**	**Escala**
Bajo	Menor a 5	
Medio	Entre 5 a 15	
Alto	Mayor a 15	

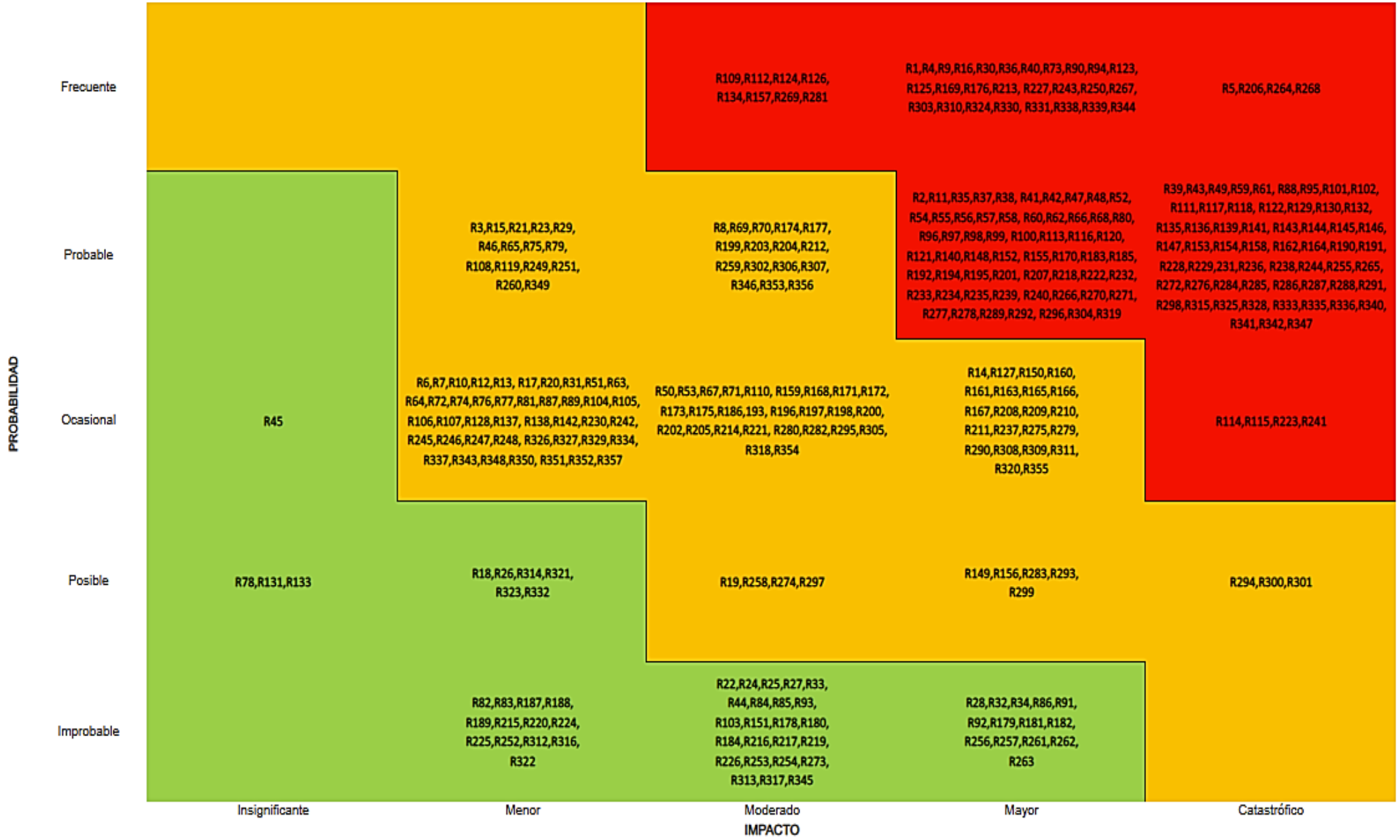
ANÁLIS DE RIESGO

ACTIVO	ASUMIR RIESGO		MITIGAR RIESGO	TOTAL GENERAL	Porcentaje
	BAJO	MEDIO	ALTO		
Banner	10	16	8	34	9,52%
BDD Banner	1	5	16	22	6,16%
BDD EDUCATIVA	1	6	16	23	6,44%
EDUCATIVA	9	16	12	37	10,36%
ESPEMATICO	8	11	18	37	10,36%
Monitoreo y seguridad (Laboratorios y aulas)	3	8	25	36	10,08%
PENTAHO	9	16	12	37	10,36%
QUIPUX	8	16	13	37	10,36%
BDD QUIPUX	1	6	16	23	6,44%
Red ESPE	2	16	16	34	9,52%
Workflow	8	17	12	37	10,36%
TOTAL RIESGOS	60	133	**164**	**357**	**100%**
	193				



RIESGOS NIVEL ALTO

MAPA DE RIESGOS



DISEÑO SGSI

ESTRUCTURA ORGANIZACIONAL

Las responsabilidades de cada proceso en la organización para la seguridad de la información en el proceso de Gestión de Docencia permitirán interactuar y compartir información relevante de cada área. Durante este procedimiento se reflejará las funciones de planificación e implementación del SGSI, los procesos de verificación y monitoreo para su posterior registro.

PLAN DE TRATAMIENTO DE RIESGO

Selección de controles

Los objetivos de control se han especificado durante la planificación, su propósito es la mitigación de riesgos, apoyo en sectores específicos según lo requiera el plan de tratamiento para riesgos; para las opciones de tratamiento se tomarán en cuenta los establecidos en la norma NTE INEN ISO/IEC 27001 en el Anexo A (Referencia de objetivos de control y controles).

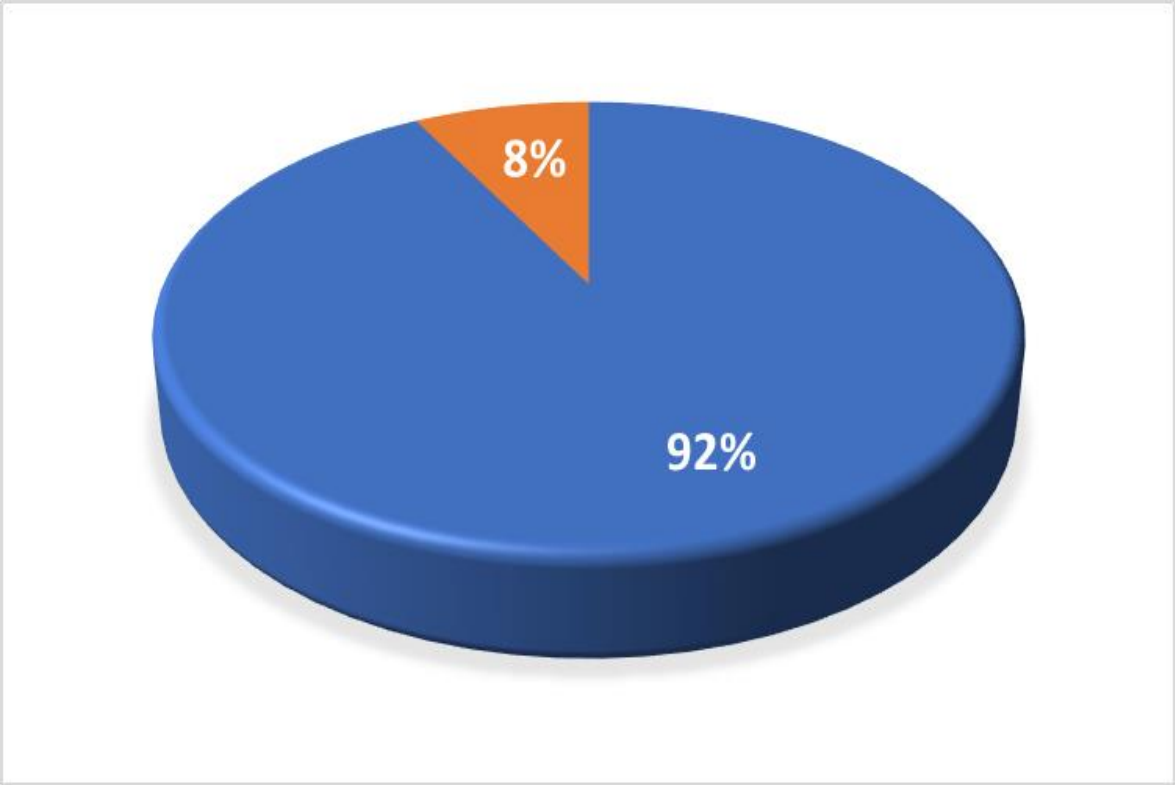
PLAN DE TRATAMIENTO DE RIESGO

Selección de controles-Declaración de aplicabilidad

114 Controles

105 controles

9 controles

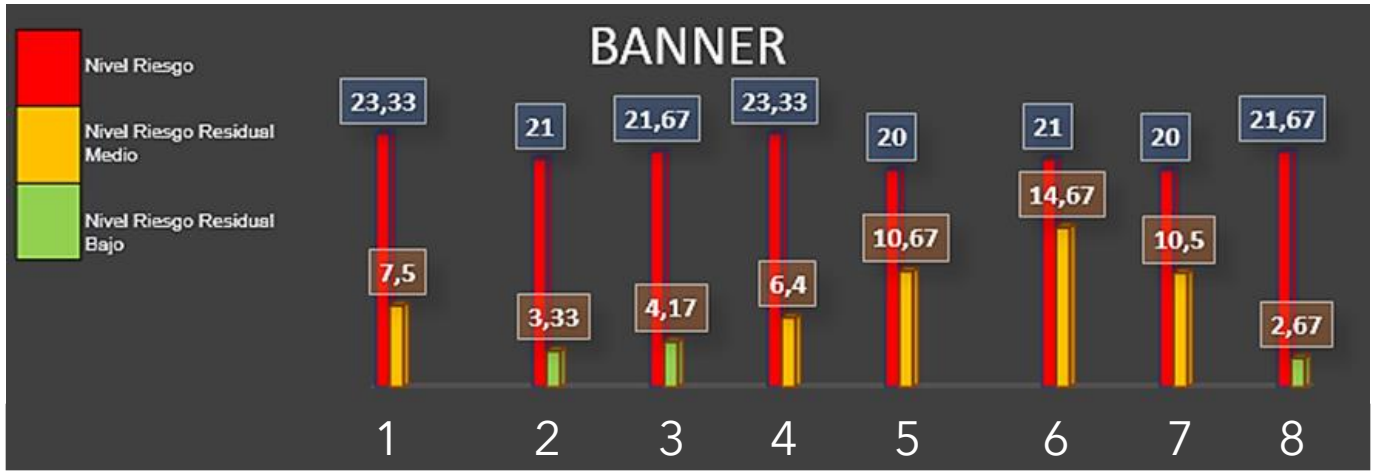


SITUACIÓN ACTUAL

- Se ha identificado cada uno de las posibles vulnerabilidades y amenazas que representan un riesgo, por lo que los riesgos superiores a 15 se han realizado el tratamiento.
- Se ha requerido de los registros de incidentes que representa la documentación donde se detalla cada actividad durante el análisis, gestión y recuperación de los activos.

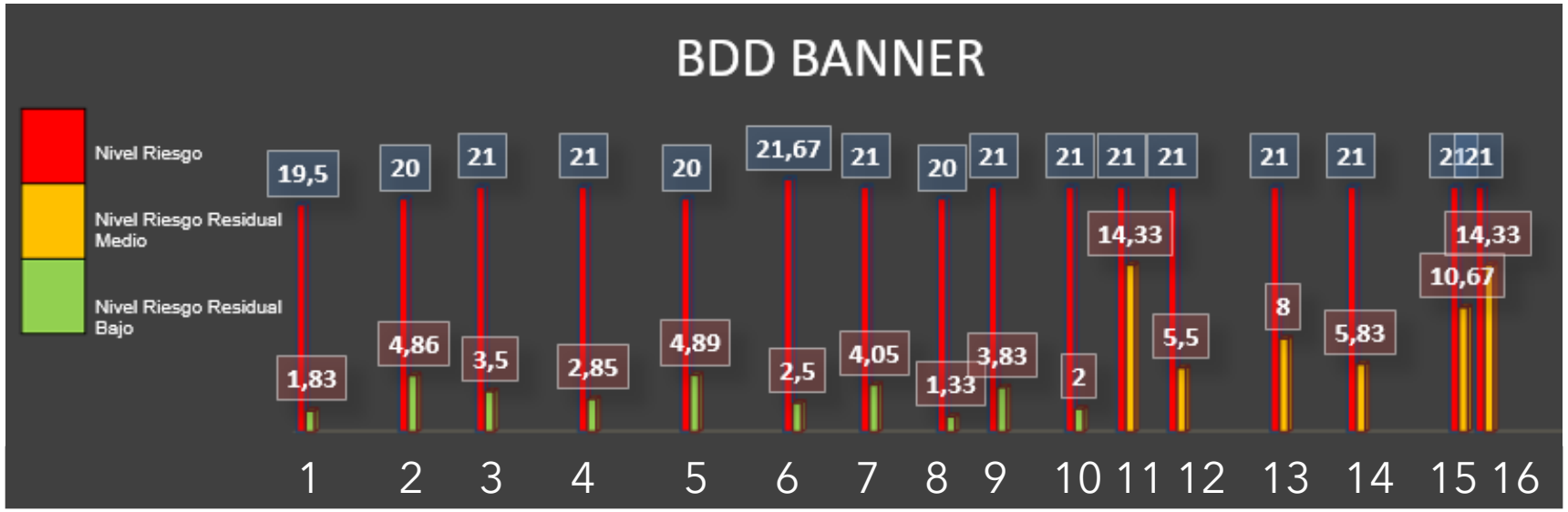
Proceso	Nivel de Riesgo
Admisión y Registro	ALTO
Control y Seguimiento Académico	MEDIO
Desarrollo Educativo	ALTO
Desarrollo Docente	MEDIO
Educación a Distancia	MEDIO
Educación Presencial	ALTO
Gestión de formación estudiantil	ALTO

Nivel de Riesgo Residual Banner



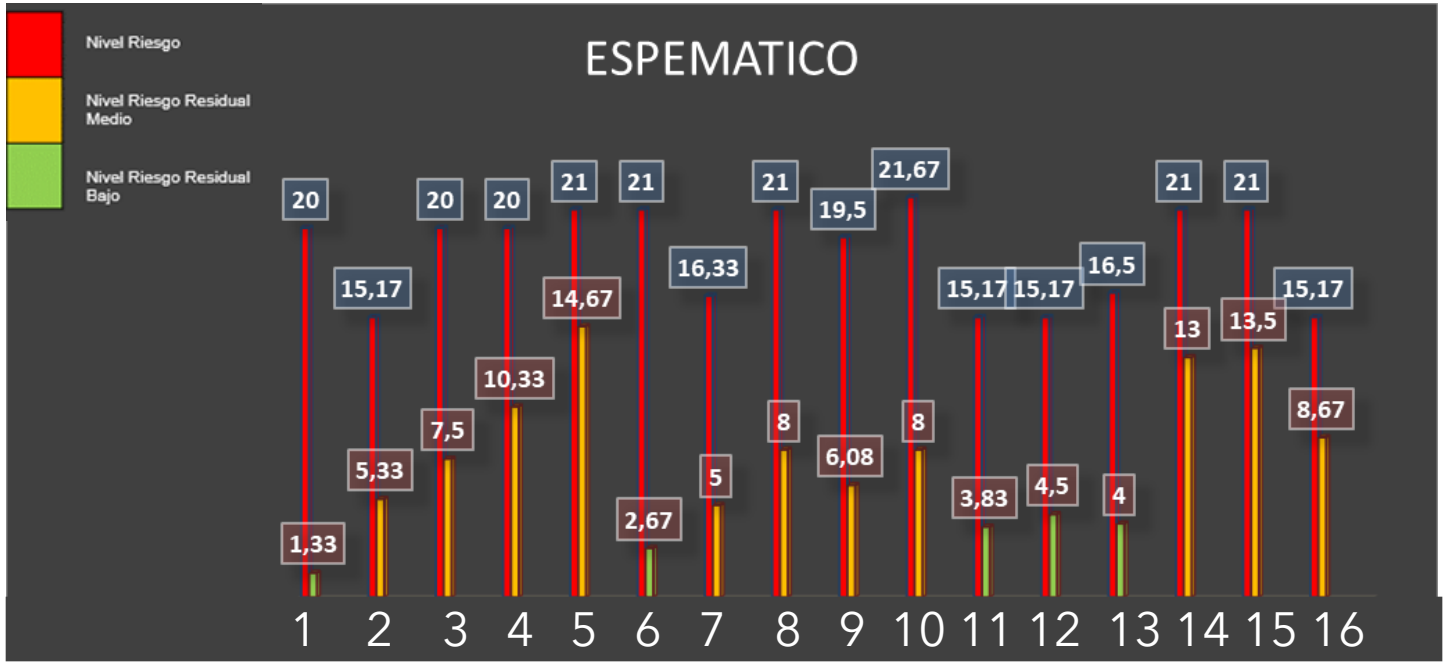
1. Mala configuración de parámetros
2. Falta de documentación
3. Falta de pistas y evidencia en auditoria
4. Asignación equivocada de los derechos de acceso
5. Distribución y/o reutilización de medios de almacenamiento sin un correcto proceso de borrado
6. Falta de atención en la disposición final
7. Amplia distribución del software
8. Falta de procedimientos de control de cambios

Nivel de Riesgo Residual Base de Datos Banner



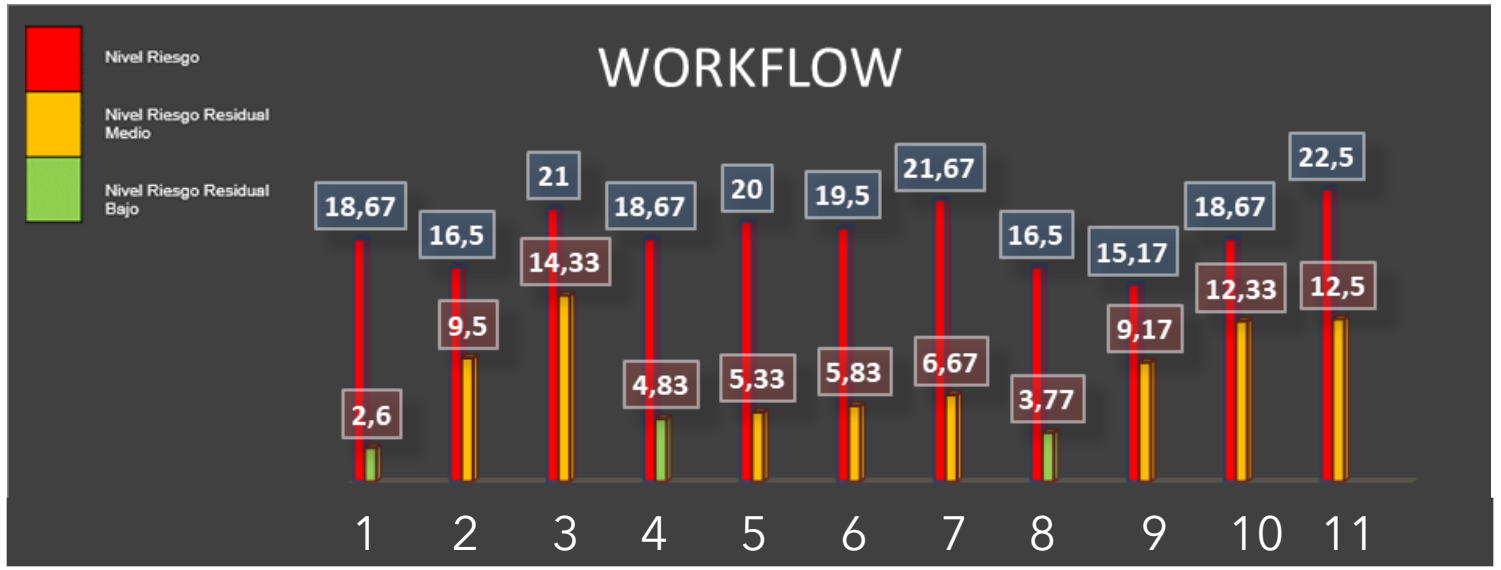
1. Falta de pistas y evidencia en auditoria
2. Asignación equivocada de los derechos de acceso
3. Defectos conocidos en el software
4. Falta de pruebas de software
5. Omisión de la acción "finalización de sesión" al abandonar la estación de trabajo
6. Distribución y/o reutilización de medios de almacenamiento sin un correcto proceso de borrado
7. Mala configuración de parámetros
8. Interfaz de usuario compleja
9. Falta de documentación
10. Amplia distribución del software
11. Uso de datos equivocados en los programas de aplicación con respecto al tiempo
12. Disposición de servicios que no se necesitan
13. Error en la producción de informes de gestión
14. Deficiencia en la gestión de contraseñas
15. Tablas de credenciales sin protección
16. Falta de procedimientos en la identificación y autentificación

Nivel de Riesgo Residual ESPEMATICO



1. Mala configuración de parámetros
2. Accesos no autorizados al sistema
3. Falta de control eficiente de cambios
4. Falta de control eficaz en cambios en la configuración
5. Falta de documentación
6. Falta de pistas y evidencia en auditoria
7. Arquitectura insegura de la red
8. Falta de acuerdos a nivel de servicio
9. Asignación equivocada de los derechos de acceso
10. Falta de procedimientos de control de cambios
11. Defectos conocidos en el software
12. Falta de pruebas de software
13. Omisión de la acción "finalización de sesión" al abandonar la estación de trabajo
14. Distribución y/o reutilización de medios de almacenamiento sin un correcto proceso de borrado
15. Falta de atención en la disposición final
16. Transferencia de credenciales en claro

Nivel de Riesgo Residual WorkFlow



1. Mala configuración de parámetros
2. Falta de documentación
3. Falta de control eficaz en cambios en la configuración
4. Falta de pistas y evidencia en auditoria
5. Falta de procedimientos de control de cambios
6. Falta de acuerdos a nivel de servicio
7. Falta de control eficiente de cambios
8. Asignación equivocada de los derechos de acceso
9. Amplia distribución del software
10. Falta de atención en la disposición final
11. Distribución y/o reutilización de medios de almacenamiento sin un correcto proceso de borrado

RESULTADO

Finalizado el proceso de tratamiento, se tiene los procesos de Gestión de Docencia con los siguientes niveles de riesgo:

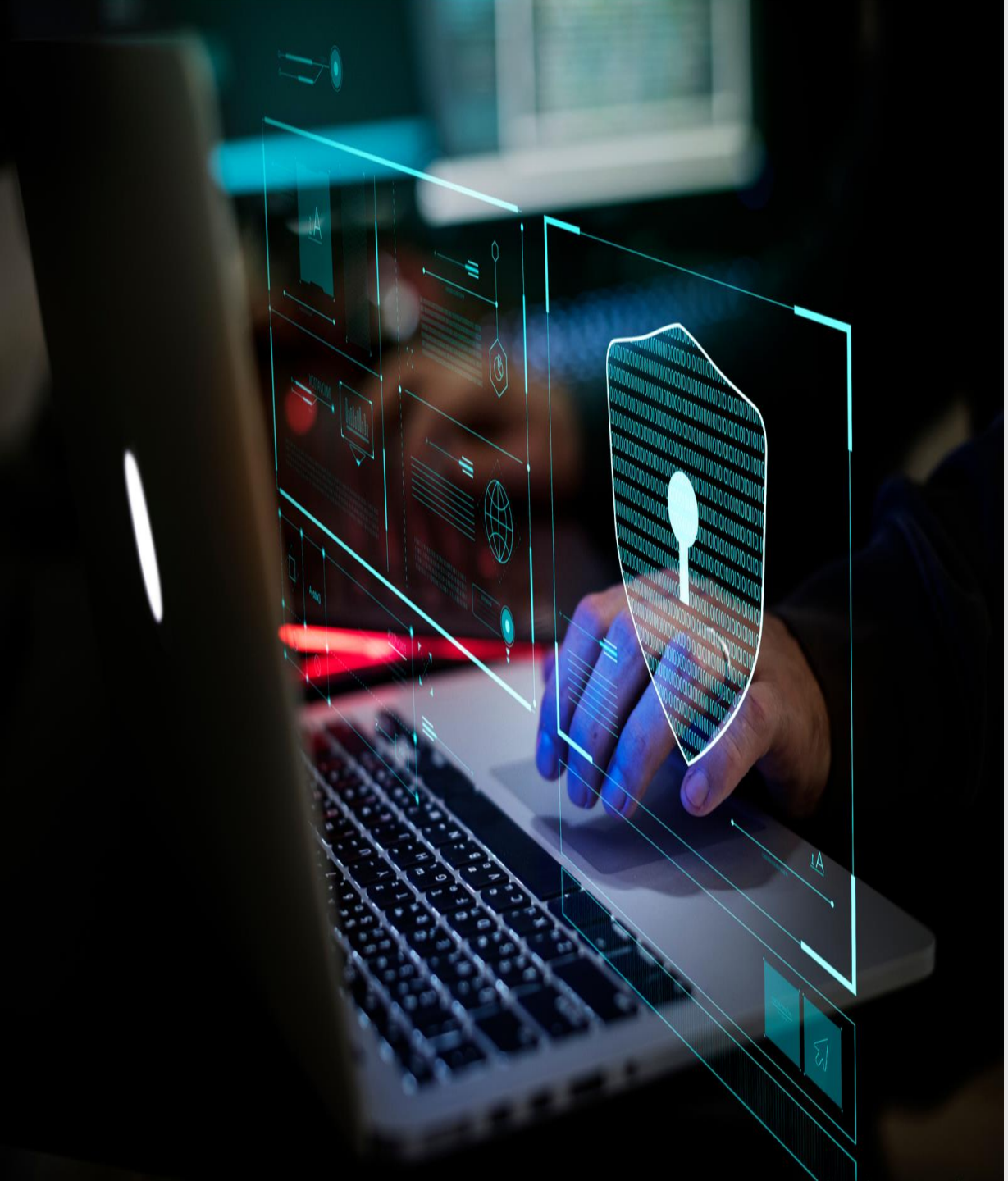
Proceso	Nivel de Riesgo
Admisión y Registro	MEDIO
Control y Seguimiento Académico	MEDIO
Desarrollo Educativo	MEDIO
Desarrollo Docente	MEDIO
Educación a Distancia	MEDIO
Educación Presencial	MEDIO
Gestión de formación estudiantil	MEDIO

POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad de la Información es una referencia con la cual la Universidad de las Fuerzas Armadas "ESPE" planificará e implementará el Esquema Gubernamental de Seguridad de la Información EGSI, que permitirá emplear controles de seguridad que permitan una oportuna protección de los activos de información.

Diseño del programa de concientización sobre seguridad de la información

- Planificación
- Implementación
- Operación
- Monitoreo y Evaluación



CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- El Esquema Gubernamental de Seguridad de la información EGSI publicado en el año 2020 a través del Acuerdo Ministerial No.025-2019, se ha planteado actualizar y continuar con el proceso en su fase número 2 con el objetivo de establecer procedimientos para la seguridad de la información en la Universidad de las Fuerzas Armadas ESPE para una adecuada planificación e implementación en la institución.
- Se ha realizado el respectivo análisis en cada uno de los macroprocesos de la universidad, destacando que existió uno prioritario y de nivel crítico en el desempeño de las funciones de los procedimientos y actividades, siendo el proceso de Gestión de Docencia, el cual interviene en acciones administrativas y académicas en cada una de las sedes a nivel nacional.
- El análisis de riesgos dio como resultado un estado actual de la seguridad de la información en el proceso de Gestión de Docencia en la universidad, destacando que los servicios pueden tener un impacto negativo a corto y largo plazo si no se realiza un plan de tratamiento de riesgos.
- El tratamiento de riesgos se realizó en base a la guía ISO 27001, y junto a la declaración de aplicabilidad donde se destaca que la institución posee algunos controles implementados; es importante definir y determinar nuevos controles con el fin de que la seguridad de la información en los procesos sea óptima.

RECOMENDACIONES

- Es necesario tener evidencia para los riesgos que han sido identificados, adoptando las medidas de cifrado de datos personales que garantizan la confidencialidad, disponibilidad e integridad de la información, del mismo modo se debe tener en cuenta el mejoramiento de estrategias en todos los sectores de la Institución basados en los estándares internacionales estipulados y lograr una eficiencia en la implementación y administración en los sistemas de seguridad de la información.
- Se recomienda que, para el análisis de riesgo, se tome en consideración las normas ISO 27001, ISO 27003, ISO 27005 con sus respectivos anexos para realizar un correcto proceso de identificación de vulnerabilidades, amenazas que puedan existir.
- Se recomienda que para el plan de tratamiento de riesgos se use los controles existentes que brinda la norma ISO 27002 en su Anexo A para un correcto procedimiento en cada uno de los riesgos encontrados durante el análisis.
- Para el procedimiento de implantación de controles, se recomienda verificar el alcance establecido junto con la política de seguridad de la información, con la finalidad de elaborar un plan de tratamiento que especifique los métodos que se utilizarán durante el proceso y ser la base de una correcta declaración de aplicabilidad.