

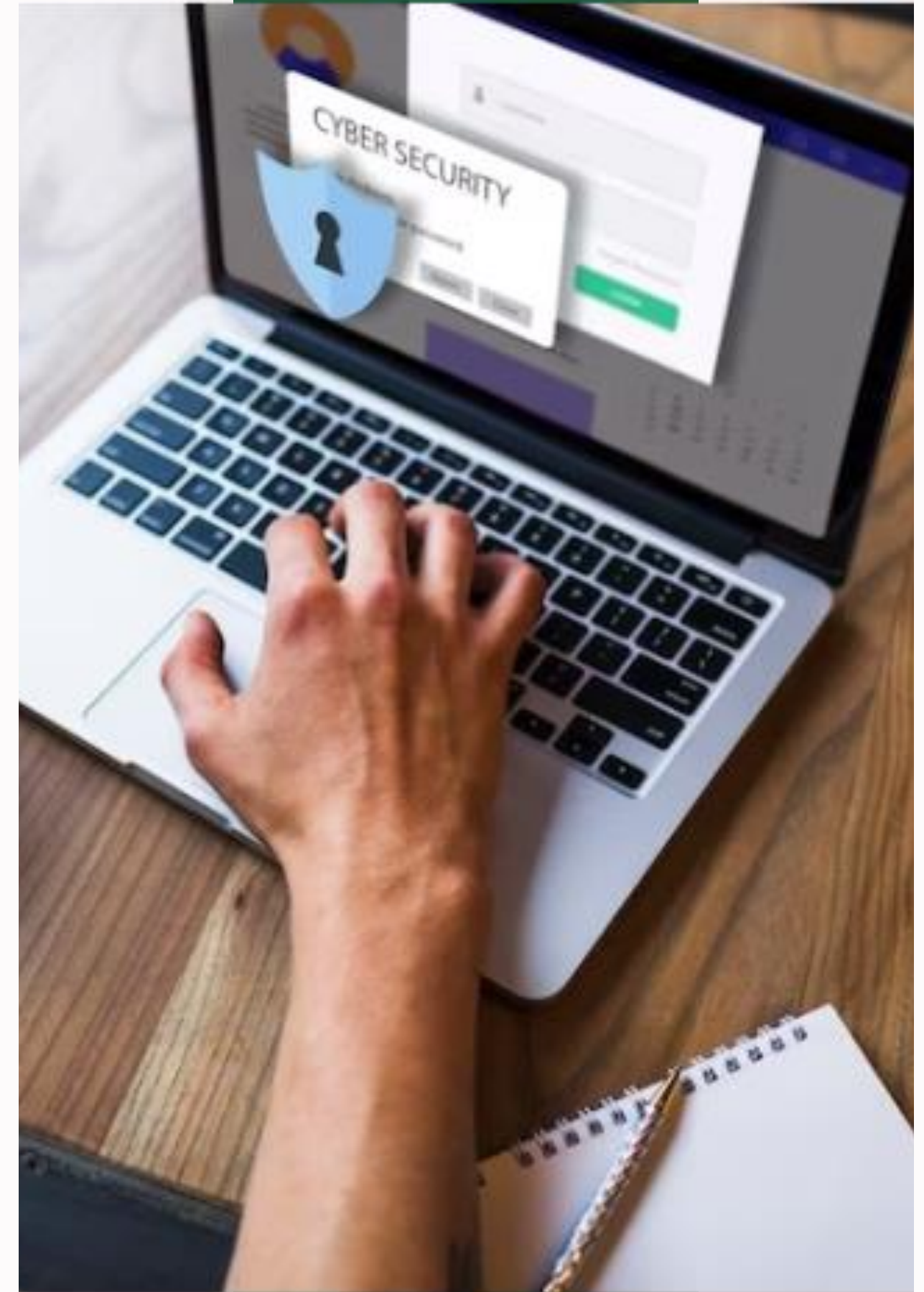


ACONDICIONAMIENTO DEL EGSÍ V2 DE LA ESPE PARA EL CUMPLIMIENTO DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES

Carrera de Tecnologías de la Información

Gerson Steven Bombón Toca

Defensor



Contenido

- 01 Introducción
- 02 Objetivos
- 03 Definiciones
- 04 Metodología
- 05 Resultados
- 06 Conclusiones y Recomendaciones
- 07 Preguntas



Introducción

El EGSI vigente de la ESPE v2 tiene eficacia, pero necesita introducir los nuevos lineamientos de la LOPDP establecidos en Acu. Minis. 025-2021

Antecedentes

Problema

La gestión, el almacenamiento y la transmisión de información, no cuentan con protección dedicada hacia datos personales y en caso de vulneración la institución podría ser demandada según la ley.

Actualización del EGSI mediante una evaluación de riesgos para así crear un plan con controles necesarios para cumplir con la LOPDP en los procesos correspondientes.

Justificación

Objetivos

Estado del Arte



Análisis de Riesgos



Tratamiento de riesgos y definición de salvaguardas



Plan de Implementación



Realizar el acondicionamiento del ESGI en base a normas ISO 27001, con el fin de proteger la información sensible en procesos internos de la ESPE

Definiciones

EGSI

Esquema Gubernamental de Seguridad de la Información

Marco regulatorio que establece los requisitos mínimos de seguridad que deben cumplir las entidades del sector público ecuatoriano para proteger la información que gestionan.

ISO 27001

Norma internacional que establece requisitos para un sistema de gestión de seguridad de la información.

Esta norma ayuda a las organizaciones a proteger la confidencialidad, integridad y disponibilidad de sus activos de información.

LOPDP

Ley Orgánica de Protección de Datos Personales

Esta ley protege los derechos de las personas sobre sus datos personales, regulando su tratamiento por parte de empresas y organizaciones.

Metodología PHVA



- Mejoras Continuas
- Optimización de procesos
- Adaptación de los procesos a los avances tecnológicos

PLANEAR



Definición de activos

10 en total
Selecc:
Banner



Mapeo de procesos internos

6
procesos
en total

Admisión y Matrícula

- Pagos
- Evaluación y Seg Académico
- Gest. Talento Humano
- Gest. Administrativa
- Gest. Medica Intitucional



Mapeo de datos personales

35 mencionados
22 seleccionados (nominativo sensible y no sensible)
(art. 4. "...datos que generan discriminación...")

HACER



Amenazas y Vulnerabilidades

Amenaza: Peligro o riesgo de que ocurra un daño o un evento no deseado.

Vulnerabilidad: Debilidad o fallo en un sistema que lo hace susceptible a un ataque o daño.

TOTAL: **39 VULNERABILIDADES**



Análisis de Riesgos

Impacto:

- Económico
- Daño Psicológico
- Img. Institucional
- Reputación personal

Probabilidad:

- Repeticiones Anuales
- Referencia Estadística
- Predicible

| | |
|---------------------|---------------------------|
| Impacto | 5 Catastrófico 1 Bajo |
| Probabilidad | 5 Certeza 1 Improbable |



Evaluación de Riesgos

IMPACTO



PROBABILIDAD

| Niveles de riesgo | Rango | Conteo |
|-------------------|--------------|-----------|
| Alto | Mayor de 12 | 24 |
| Medio | Entre 9 y 12 | 13 |
| Bajo | Menor que 9 | 2 |

EVALUACIÓN DE RIESGOS

| Activo | Amenaza | Vulnerabilidades | Impacto (consecuencia, daño) | Probabilidad % | Valoración | | | | | | | | Nivel de Riesgo | |
|--------|---|--|---|----------------|------------|------|------|-----|-------|--------------|----|----|-----------------|-------|
| | | | | | Impacto | | | | | Probabilidad | | | | |
| | | | | | Ec | Psic | ImIn | Rep | Total | RA | RE | OT | | Total |
| Banner | Evento natural (Inundación, tormenta eléctrica, sismo) | centro de cómputo bajo nivel probable de inundación -- Protección hasta sismo grado 8) | suspensión de servicio | 30 | 3 | 3 | 4 | 2 | 3 | 4 | 2 | 5 | 3,67 | 11,00 |
| | Abuso de derechos | permite descargar e imprimir calificaciones de los alumnos | divulgación y pérdida de integridad de los datos | 90 | 2 | 4 | 3 | 5 | 3,5 | 4 | 5 | 4 | 4,33 | 15,17 |
| | Intrusos o personal malicioso no autorizado | mecanismos de identificación y autenticación no adecuados | acceso no autorizado a la cuenta del titular con posible divulgación de información personal mediante ataques de fuerza bruta | 95 | 4 | 5 | 3 | 5 | 4,25 | 4 | 5 | 3 | 4,00 | 17,00 |
| | | gestión y uso deficiente de contraseñas | acceso no autorizado a la cuenta del titular con posible divulgación de información personal | 95 | 2 | 5 | 3 | 5 | 3,75 | 2 | 5 | 3 | 3,33 | 12,50 |
| | Error en el diseño del software (capacidad y tiempo de respuesta) | gestión inadecuada de la infraestructura | suspensión de servicio | 70 | 2 | 2 | 2 | 2 | 2 | 5 | 4 | 2 | 3,67 | 7,33 |
| | | defectos en el diseño y construcción del software | suspensión de servicio que afecta a procedimientos sensibles | 80 | 4 | 3 | 2 | 3 | 3 | 3 | 4 | 3 | 3,33 | 10,00 |

Ejemplo tomado del Anexo A

VALIDAR



Controles y Salvaguardas

| Estrategia | | | |
|--------------|--------------|--------|----------------|
| Nivel Riesgo | Rango | Color | Opción |
| Alto | Mayor de 12 | Red | Reducir Riesgo |
| Medio | Entre 9 y 12 | Yellow | Aceptar Riesgo |
| Bajo | Menor que 9 | Green | |



Riesgos a reducir: **24**

Riesgos a aceptar: **15**



Riesgo Residual

IMPACTO Res.



PROBABILIDAD Res.



Objetivo:
Riesgos nivel Medio

EVALUACIÓN DE RIESGO RESIDUAL

| Activo | Amenaza | Vulnerabilidades | Riesgo Inh. | Controles y Salvaguardas | Evaluación Residual | | | | | | | | Riesgo Residual | |
|--------|---|--|-------------|--|---------------------|------|------|-----|-------|------------------|----|----|-----------------|-------|
| | | | | | Impacto res | | | | | Probabilidad res | | | | |
| | | | | | Ec | Psic | ImIn | Rep | Total | RA | RE | OT | | Total |
| Banner | Evento natural (Inundación, tormenta eléctrica, sismo) | centro de cómputo bajo nivel probable de inundación -- Protección hasta sismo grado 8) | 11,00 | | | | | | | | | | | |
| | Abuso de derechos | permite descargar e imprimir calificaciones de los alumnos | 15,17 | Definir una política para controlar la manipulación de información personal sensible con sus respectivas sanciones | 4 | 1 | 4 | 1 | 2,50 | 4 | 5 | 4 | 4,33 | 10,83 |
| | Intrusos o personal malicioso no autorizado | mecanismos de identificación y autenticación no adecuados | 17,00 | Implementar el mecanismo de seguridad de multifactor de autenticación | 3 | 2 | 3 | 3 | 2,75 | 4 | 5 | 3 | 4,00 | 11,00 |
| | | gestión y uso deficiente de contraseñas | 12,50 | Definir política de gestión y uso de contraseñas seguras para todos los titulares de la universidad | 2 | 3 | 3 | 3 | 2,75 | 2 | 5 | 3 | 3,33 | 9,17 |
| | Error en el diseño del software (capacidad y tiempo de respuesta) | gestión inadecuada de la infraestructura | 7,33 | | | | | | | | | | | |
| | defectos en el diseño y construcción del software | 10,00 | | | | | | | | | | | | |

Ejemplo tomado del Anexo A

ACTUAR



Plan de implementación

- **Actividades**

Serie de pasos propuestos para cumplir con el control establecido

- **Tiempo estimado**

| Tiempo Estimado | |
|--------------------------|------------|
| SUMATORIO: | 84 semanas |
| REDUNDANCIA DE CONTROLES | 44 semanas |
| TOTAL | 40 semanas |

- **Presupuesto estimado**

| Presupuesto Económico Estimado | |
|--------------------------------|-------------|
| SUMATORIO: | \$30.200,00 |
| REDUNDANCIA DE CONTROLES | \$16.000,00 |
| TOTAL | \$14.200,00 |



Plan de
implementación

- **Indicadores**

- **Eficacia:** Lograr el objetivo deseado.
- **Eficiencia:** Lograr el objetivo utilizando la menor cantidad de recursos posible.
- **Frecuencia:** Cuántas veces se mide el progreso hacia el objetivo.

- **Responsabilidad**

Será el designado o responsable de cada activo

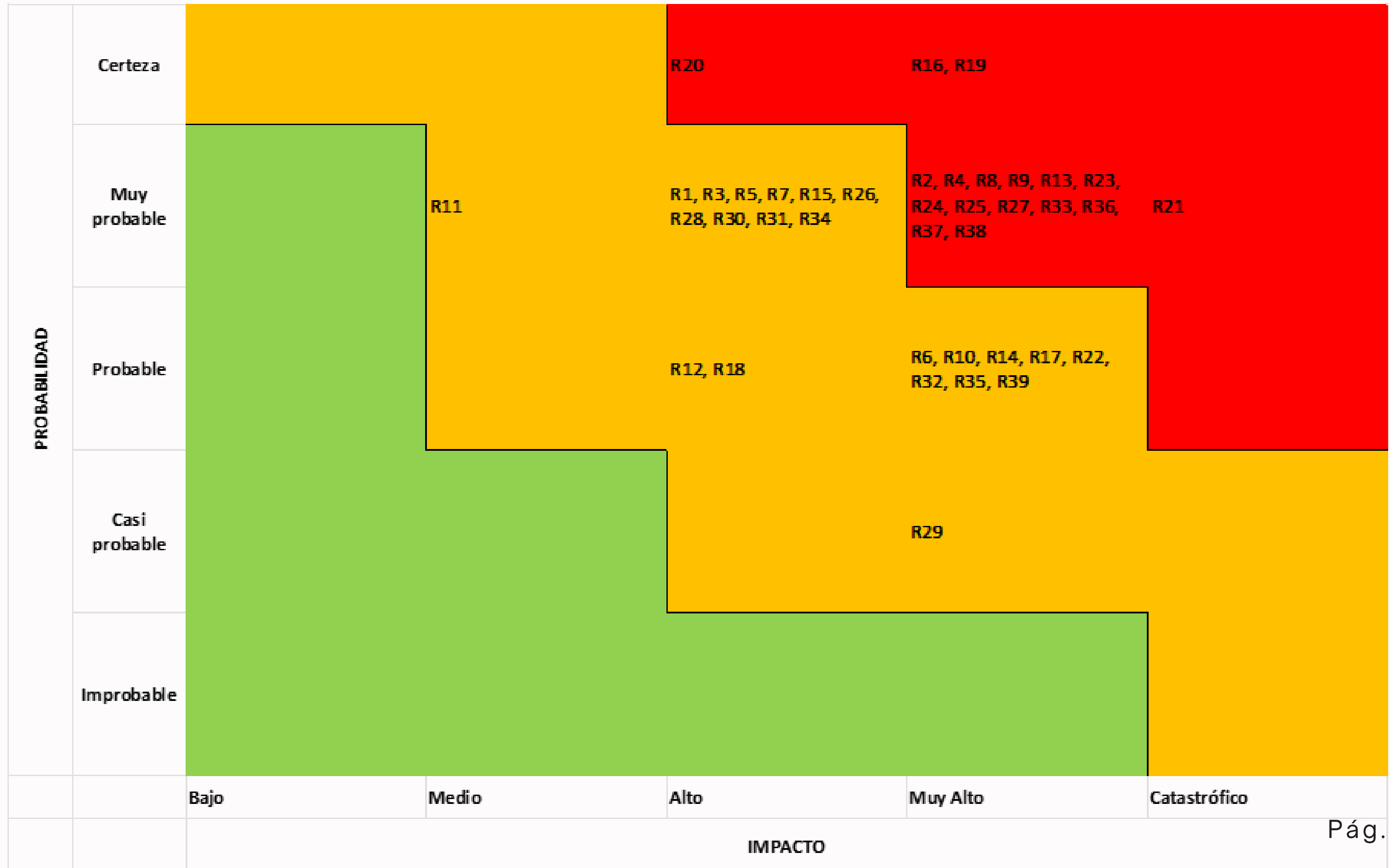
Plan de implementación

| Activo | Vulnerabilidades | Riesgo Inh. | Controles y Salvaguardas | Riesgo Residual | Implantación | | | | | | |
|--------|--|-------------|--|-----------------|---|---------------------------|-------------|--|--|------------------------|--------------------------|
| | | | | | ACTIVIDADES | Tiempo de plazo (semanas) | Presupuesto | INDICADORES DE EVALUACION | | | Responsables |
| | | | | | | | | Eficiencia | Eficacia | Frecuencia de medición | |
| Banner | centro de cómputo bajo nivel probable de inundación -- Protección hasta sismo grado 8) | 11,00 | | | | | | | | | |
| | permite descargar e imprimir calificaciones de los alumnos | 15,17 | Definir una política para controlar la manipulación de información personal sensible con sus respectivas sanciones | 10,83 | 1. Redacción de la política, 2. Aprobación de la política por la alta dirección. 3. Capacitación al personal sobre la política. 4. Implementación de la política. | 4 semanas | \$1.000,00 | Porcentaje de información personal sensible protegida | Porcentaje de casos de manipulación de información personal sensible | Anual | Luis Gonzalo Rocha Hoyos |
| | mecanismos de identificación y autenticación no adecuados | 17,00 | Implementar el mecanismo de seguridad de multifactor de autenticación | 11,00 | 1. Evaluación de las opciones de MFA disponibles. 2. Selección de la solución MFA más adecuada. 3. Implementación de la solución MFA. 4. Capacitación al personal sobre el uso de MFA. | 4 semanas | \$2.000,00 | Porcentaje de usuarios que utilizan la autenticación multifactor | Porcentaje de intentos de acceso no autorizado al sistema | Trimestral | |
| | gestión y uso deficiente de contraseñas | 12,50 | Definir política de gestión y uso de contraseñas seguras para todos los titulares de la universidad | 9,17 | 1. Redacción de la política. 2. Aprobación de la política por la alta dirección. 3. Capacitación al personal sobre la política. 4. Implementación de la política. | 3 semanas | \$500,00 | Porcentaje de usuarios con contraseñas seguras | Porcentaje de casos de acceso no autorizado al sistema por contraseñas débiles | Semanal | |
| | gestión inadecuada de la infraestructura | 7,33 | | | | | | | | | |
| | defectos en el diseño y construcción del software | 10,00 | | | | | | | | | |
| | | | | | | | | | | | |

Ejemplo tomado del Anexo A

RESULTADOS

Mapa de Riesgos sin tratamiento LOPDP



Mapa de Riesgos con tratamiento LOPDP



CONCLUSIONES

Estado del Arte



Se logró un buen análisis mediante la investigación, obteniendo los datos personales que deben ser tratados.

Análisis de Riesgos



Se realizó un análisis de riesgos con detalles muy granuales ya que partimos de vulnerabilidades reales.

Tratamiento de Riesgos



Se realizó un tratamiento de riesgos consistentes, estableciendo controles y salvaguardas correspondientes a cada una de las vulnerabilidades.

Plan de Implementación



Se planteó un plan detallado donde se detalló actividades e indicadores de eficiencia para su evaluación.

RECOMENDACIONES



Implementación correcta

Apegarse a la planificación planteada ya que son controles y salvaguardas recomendados son los mas apegados a la realidad.



Uso de PHVA para la evaluación

Mediante el uso de la metodología mencionada y los indicadores planteados evaluar y mejorar los salvaguardas de la información.



Concienciación

“El factor humano es el eslabón más débil de la cadena de ciberseguridad, por eso la formación es el elemento mitigador más eficaz para erradicar el riesgo...”

- Albert Salvador, Secretario General Internacional de la WCA.

Equipo de Trabajo



Steven
Bombón
Defensor







Mario
Ron
Tutor



THANK YOU ESPE

Steven Bombón

-  +593 998 141 994
-  steven.bombon@icloud.com
-  n9.cl/gsbombon-lnkdn
-  Quito, Ecuador

