UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN TELECOMUNICACIONES

MENCIÓN: GESTIÓN DE LAS TELECOMUNICACIONES

Resolución: RPC-SE-01-No.016-2020

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGISTER

Título del proyecto:
Creación de una política de seguridad de la información para una empresa de Telecomunicaciones
Línea de Investigación:
Telecomunicaciones y Sistemas Informáticos aplicados a la producción y la sociedad
Campo amplio de conocimiento:
Tecnologías de la información y Comunicación (TIC)
Autor:
Ing. Jaime Xavier Caiza Tipán
Tutor:
PhD Wilmer Fabián Albarracín Guarochico

Quito – Ecuador

2021

APROBACIÓN DEL TUTOR

Yo, PhD Wilmer Albarracín con C.I: 1713341152, en mi calidad de Tutor del proyecto de investigación titulado: Creación de una política de seguridad de la información para una empresa de Telecomunicaciones.

Elaborado por: Jaime Xavier Caiza Tipán, de C.I: 1713553350, estudiante de la Maestría: Maestría en Telecomunicaciones mención: Gestión de las Telecomunicaciones mediado por TIC de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., 09 de septiembre de 2021

_____

Firma

Tabla de contenidos

APROBACIÓN DEL TUTOR ii
DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE ..... **¡Error! Marcador no definido.**
INFORMACIÓN GENERAL 1
Contextualización del tema 1
Pregunta Problemática 2
Objetivo general 2
Objetivos específicos 2
Beneficiarios directos: 2
CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO 2
1.1. Contextualización de fundamentos teóricos 2
1.2. Problema a resolver 3
1.3. Proceso de investigación 4
1.4. Vinculación con la sociedad 4
1.5. Indicadores de resultados 4
CAPÍTULO II: PROPUESTA 5
2.1. Fundamentos teóricos aplicados 5
2.1.1. Sistema de gestión de seguridad de la información (SGSI) 5
2.1.2. Ciclo de Deming 5
Planificar 5
Hacer 5
Controlar 6
Actuar 6
2.1.3. Principios 6
Confidencialidad 6
Integridad: 7
Disponibilidad 7
2.1.4. Proceso para la gestión del riesgo de la seguridad de la información 7
2.1.4.1. Establecimiento del contexto 9
2.1.4.2. Criterios básicos 9
Identificación del riesgo 9
Evaluación del riesgo 9
Impacto del riesgo 9
Aceptación del riesgo 9
Alcance y límites 10

2.2. Descripción de la propuesta 10
2.3. FASE I: FASE INICIAL 10
2.3.1. Recopilación de información 10
Población y Muestra 10
Muestra 10
Resultados de las encuestas 10
Pregunta Nro. 1 10
Interpretación 11
Pregunta Nro. 2 11
Interpretación 12
Pregunta Nro. 3 12
Interpretación 13
2.4. Fase II. DEFINICIÓN 14
2.4.1. Análisis 14
2.4.1.1. Situación Actual 14
Distribución actual área técnica 14
Planta baja - edificio administrativo 14
Primer piso - edificio administrativo 15
Planta baja - edificio área técnica 17
2.5. Fase III. EJECUCION 18
2.5.1. Desarrollo 18
2.5.1.1. Gestión del riesgo de la seguridad de la información 18
Diagrama de flujo 19
2.5.1.2. Valoración del riesgo 20
Actividades: 20
Analizar el riesgo 20
Identificar el riesgo 20
Identificar los activos 20
Primarios: 21
De soporte: 21
2.5.1.3. Valorar los activos 23
Identificación de Amenazas 26
Identificar las Vulnerabilidades 27
Identificación de Existencia de Controles 28
Estimación o Análisis del riesgo 30
Evaluación del riesgo 30

Criterios de probabilidad de ocurrencia de amenazas 30
Criterio de la Evaluación de Riesgos 31
2.5.1.4. Tratamiento del Riesgo 35
Diagrama de flujo 36
Reducir el riesgo 37
Aceptación del riesgo 37
Transferir el riesgo 38
Evitar el riesgo 38
Comunicar los riesgos 38
Monitoreo de los riesgos 38
Revisión y mejora 38
2.6. Fase IV. Política 39
2.6.1. POLÍTICA DE SEGURIDAD 39
2.6.2. Objetivo 39
2.6.3. Alcance 39
2.6.4. Responsabilidades 39
2.6.5. Procedimientos 40
2.6.5.1. Política para el computador 40
Objetivo. 40
Alcance 40
Política 40
Responsabilidad del usuario del activo 40
Controles 40
Restricciones y prohibiciones. 40
2.6.5.2. Política de la Impresora 41
Objetivo 41
Alcance 41
Política 41
Responsabilidad del usuario del activo 41
Controles 41
Restricciones y prohibiciones. 41
2.6.5.3. Política para la red de datos 41
Objetivo. 41
Alcance 42
Política: 42
Responsabilidades. 42

Controles. 42
Restricciones y prohibiciones. 42
2.6.5.4. Política para el Access Point 42
Objetivo. 42
Alcance. 42
Política: 42
Responsabilidades. 42
Controles. 43
Restricciones y prohibiciones. 43
2.6.5.5. Política para la Cámara de seguridad 43
Objetivo. 43
Alcance. 43
Política: 43
Responsabilidades. 43
Controles. 43
Restricciones y prohibiciones. 44
2.6.5.6. Política para el Cortafuego 44
Objetivo. 44
Alcance. 44
Política: 44
Responsabilidades. 44
Controles. 44
Restricciones y prohibiciones. 44
2.6.5.7. Política para el Biométrico 45
Objetivo. 45
Alcance. 45
Política: 45
Responsabilidades. 45
Controles. 45
Restricciones y prohibiciones. 45
2.6.5.8. Política para el Router de acceso principal 45
Objetivo. 45
Alcance. 46
Política: 46
Responsabilidades. 46
Controles. 46

Restricciones y prohibiciones. 46
2.6.5.9. Política para el Router de acceso secundario 46
Objetivo. 46
Alcance. 47
Política: 47
Responsabilidades. 47
Controles. 47
Restricciones y prohibiciones. 47
2.6.5.10. Política para el Antivirus 47
Objetivo. 47
Alcance. 47
Política: 48
Responsabilidades. 48
Controles. 48
Restricciones y prohibiciones. 48
2.6.5.11. Política para las Aplicaciones 48
Objetivo. 48
Alcance. 48
Política: 48
Responsabilidades. 48
Controles. 48
Restricciones y prohibiciones. 49
2.6.5.12. Política para el Servicio de correo Exchange 49
Objetivo. 49
Alcance. 49
Política: 49
Responsabilidades. 49
Controles. 49
Restricciones y prohibiciones. 49
2.6.5.13. Política para el Colaborador administrativo 50
Objetivo. 50
Alcance. 50
Política: 50
Responsabilidades. 50
Controles. 50
Restricciones y prohibiciones. 50

2.6.5.14. Política para el Colaborador técnico 50
Objetivo. 50
Alcance. 50
Política: 51
Responsabilidades. 51
Controles. 51
Restricciones y prohibiciones. 51
Fase V: Resultados 51
2.7. Matriz de articulación 52
CONCLUSIONES 53
RECOMENDACIONES 54
BIBLIOGRAFÍA 55
ANEXO 1 56
Encuestas completas con los resultados obtenidos 56

Índice de tablas

Tabla 1. Políticas Copias de seguridad 11
Tabla 2. Políticas de seguridad de la información 12
Tabla 3. Información segura 13
Tabla 4. Esquema actual Planta baja- edificio administrativo 14
Tabla 5. Distribución Primer piso - edificio administrativo 16
Tabla 6. Distribución Planta baja - edificio área técnica 17
Tabla 7. Activos identificados - edificios área técnica 18
Tabla 8. Identificación de los activos 21
Tabla 9. Valoración - confidencialidad de la información 23
Tabla 10. Valoración - Integridad de la información 24
Tabla 11. Valoración - Disponibilidad de la información 24
Tabla 12. Valoración de los activos de información 25
Tabla 13. Identificación de Amenazas 26
Tabla 14. Valoración - Activos de información 27
Tabla 15. Valoración de los activos de información 28
Tabla 16. Valoración de los activos de información 30
Tabla 17. Valoración de los activos de información 31
Tabla 18. Nivel de criterio de vulnerabilidad 32
Tabla 19. Valoración de los activos de información 33
Tabla 20. Matriz de articulación 52

Índice de figuras

Figura 1. Ciclo de Deming 5
Figura 2. Principios del SGSI 6
Figura 3. Proceso para la gestión del riesgo de seguridad de la información 8
Figura 4. Proceso de gestión del riesgo en la seguridad de la información 8
Figura 5: Copias de seguridad 11
Figura 6: Políticas de seguridad de la información 12
Figura 7: Información segura 13
Figura 8. Esquema actual Planta baja- edificio administrativo 15
Figura 9. Esquema actual Primer piso - edificio administrativo 16
Figura 10. Esquema actual Planta baja - edificio área técnica 17
*Figura 11. G*estión del riesgo de la seguridad de la información 19
Figura 12. Tratamiento del Riesgo 36

INFORMACIÓN GENERAL

Contextualización del tema

Actualmente es importante precautelar la seguridad de toda la información generada por las instituciones por ende es imprescindible estar prevenidos ante posibles ataques hacia las redes de las diferentes empresas sean grandes o pequeñas lo cual puede traer consigo una pérdida de tiempo, dinero y sobre todo robo de información o posibles daños a la información que ya se tiene almacenada, misma que en la actualidad se pueden considerar como activos importantes para una empresa.

Los atacantes buscan tener un ingreso a las redes de las empresas utilizando diferentes software mismos que buscan vulnerabilidades.

Podemos mencionar que una vulnerabilidad es una debilidad que puede estar en nuestra red o en cualquiera de los dispositivos que usamos y tienen acceso a internet o se conectan a una intranet por medio de diferentes equipos como enrutadores, servidores u otro equipo que le de dicho acceso, esto es debido a que los equipos tienen cuentas no seguras ya que el usuario es fácil de adivinar o las contraseñas no son robustas, también se puede decir que los servicios en los enrutadores no está configurados de manera adecuada o tiene las configuraciones predeterminadas, todo lo antes mencionado se puede mitigar si se genera una política de seguridad adecuada misma que se debe cumplir por todos los colaboradores y cumpla con ciertos parámetros de autenticación, controles de acceso tanto físicos como lógicos, políticas de seguridad a nivel de software y hardware, así como los usuarios de los equipos de la empresa sean en base a los perfiles y no tengan libre administración de los mismos.

Los equipos que sufren más ataques actualmente son los computadores de escritorio, portátiles o en algunos de los casos los servidores.

Si los equipos pueden ser vulnerados es importante contar con una política de respaldo de la información para mitigar una posible pérdida de la información y evitar que sean afectados todos y cada uno de los activos de la institución.

Por todo lo expuesto anteriormente se debería definir una política de seguridad de la información para poder abordar las vulnerabilidades de los activos en las diferentes empresas de Telecomunicaciones.

Pregunta Problemática

¿La creación de una política de seguridad de la información fundamentada en las normativas de seguridad de la información vigentes, nos ayudara a proteger y resguardar la información que se genera y almacena en una empresa de Telecomunicaciones?

Objetivo general

Creación de una política para la seguridad de la información la cual nos ayudara a proteger y resguardar los datos e información generada en una empresa de Telecomunicaciones fundamentada en las normativas de seguridad de la información vigentes.

Objetivos específicos

- Establecer el marco teórico sobre la gestión del riesgo de seguridad de la información, en base a las normativas de seguridad de la información vigentes.
- Evaluar el riesgo para la seguridad de la información mediante el análisis, identificación y estimación del riesgo.
- Desarrollar el tratamiento del riesgo para la seguridad de la información mediante la reducción, aceptación, transferencia y comunicación del mismo.
- Diseñar los procesos de una política de seguridad de la información, de acuerdo a las normativas de seguridad de la información vigentes que permitan garantizar la confidencialidad, disponibilidad e integridad de la información.

Beneficiarios directos:

Los beneficiarios directos con la definición de una política de seguridad de la información en una empresa de telecomunicaciones, son todos los colaboradores que trabajan en la empresa descrita, quienes podrán proteger y resguardar los datos la información de un modo más organizado, confiable y seguro.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

1.1. Contextualización de fundamentos teóricos

A medida que se trabaja en el entorno de la seguridad de los datos y de la información, nos vemos en la necesidad de difundir la educación en estos tópicos; sin embargo, en espacios educativos o profesionales no basta con aplicar un antivirus en un computador personal o laboral, tampoco es suficiente por ejemplo proteger su teléfono celular de la sustracción de la información. Por ello, es necesario buscar documentos y lineamientos que nos guíen cómo plantear la seguridad con una

metodología de forma responsable y orientada para cumplir los mínimos estándares que se requieren para manejar la actual tecnología.

Según la ISO/IEC (2016),"la seguridad de la información se podría definir como aquellos procesos, buenas prácticas y metodologías que busquen proteger la información y los sistemas de información del acceso, uso, divulgación, interrupción, modificación o destrucción no autorizada. Esta definición nos indica que debemos proteger nuestros datos, nuestra información y nuestros recursos de infraestructura tecnológica de aquellos quienes intentarían hacer un mal uso de estos". (ISO/IEC, 2016)

El principal objetivo de la ISO 27002 es "establecer directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Esto también incluye la selección, implementación y administración de controles, teniendo en cuenta los entornos de riesgo encontrados en la empresa (INEN, 2012)".

Según Vidalina De Freitas Fern Ndez (2012), en su libro" Sistema de Gestión de Seguridad de la Información" hace referencia a la falta de seguridad en la información, "Hoy en día, las organizaciones o empresas son cada vez más dependientes de las redes informáticas por lo que un problema que las afecte, por más pequeño que sea, podría llegar a comprometer seriamente la continuidad de sus operaciones. La falta de medidas o política de seguridad en las redes es un serio problema ya que cada vez más aumenta el número de atacantes y éstos a su vez están más organizados adquiriendo habilidades especializadas que les permiten una mayor probabilidad de éxito. Por ello, se debe identificar, analizar, evaluar y gestionar los posibles riesgos a los que se enfrentan los activos de información de una organización, con la finalidad de disminuir, o en el mejor de los casos, eliminar su posible ocurrencia. Las Normas ISO 27001, proporciona una excelente guía para gestionar los recursos de las organizaciones, en particular, recomienda la implantación de un Sistema que permita gestionar la seguridad de sus activos y poder contar con mecanismos de recuperación de sus operaciones, en caso de llegarse a materializar algunas de ellas." De esta manera, nos da pie a la necesidad de la creación de una política de seguridad de la información que incluya las normativas recomendadas en la ISO 27001 e ISO 27002. (Fern, 2012)

1.2. Problema a resolver

Actualmente la empresa de telecomunicaciones, no cuenta con una política de seguridad de la información, la cual se ha trasformado en los últimos tiempos en un requisito primordial en las empresas e instituciones tanto públicas como privadas convirtiéndose en un bien de consumo para ellas. Por esta razón es importante familiarizarse con el término Seguridad de la Información la cual

se determinó por el elevado número de incidentes de seguridad ocurridos en las empresas en todo el mundo.

El incremento en de nuevas tecnologías y aplicativos de información y por ende el uso en la empresa de telecomunicaciones, ha ocasionado fisuras o brechas en términos de seguridad con relación a su empleo, en consecuencia, se hace necesario crear una política relacionada a la seguridad de la información que sirva para la empresa, considerando las normativas de seguridad de la información vigentes.

1.3. Proceso de investigación

La metodología que utilizaremos será una investigación de campo, en vista de que la información que se recolectará será tomada de las experiencias diarias de los colaboradores de la empresa que hacen uso de las tecnologías de la información actuales.

Se empleará un esquema descriptivo transaccional, no experimental, la variable e indicadores serán observados en circunstancias naturales, esto es, se desplegará las mediciones de las variables operacionales para lograr los objetivos propuestos, sin que estos puedan ser cambiados, modificados u alterados por terceras personas.

1.4. Vinculación con la sociedad

Con la creación de una política para la seguridad de la información que se implementara en una empresa de telecomunicaciones, estamos protegiendo y dando seguridad a la información y a los datos, considerando las normativas de seguridad de la información vigentes, ofreciendo una ventaja competitiva mayor, asignando y estableciendo obligaciones, roles y responsabilidades definidas para un mejor desempeño y funcionamiento de una empresa; este documento servirá de guía para estudiantes, profesionales y empresas de telecomunicaciones que requieran resguardar y proteger sus activos de información considerando las normativas de seguridad de la información vigentes.

1.5. Indicadores de resultados

Los indicadores de resultados será la evaluación de los riesgos de los activos una vez creada he implantada una política para la seguridad de la información en una empresa de Telecomunicaciones, los resultados que se espera obtener denotaran grandes mejoras en la seguridad de la información de sus activos y minimizara las vulnerabilidades que estén afectando la seguridad de la información, y de esta manera, avalar los objetivos planteados.

CAPÍTULO II: PROPUESTA

2.1. Fundamentos teóricos aplicados

2.1.1. Sistema de gestión de seguridad de la información (SGSI)

Es un conjunto de reglamentos y normativas para la gestión de la información.

La terminología SGSI es un estándar internacional utilizada por la ISO/IEC 27001, que fue aprobada en octubre de año 2005 a través de la comisión International Electrotechnical Commission y la International Organización for Standardization

La ISO/IEC 27001 define las disposiciones necesarias la cuales nos ayudan a implantar, establecer y mantener una mejora continua del Sistema de Gestión de la Seguridad de la Información (SGSI) en una empresa o institución.

2.1.2. Ciclo de Deming

Se identifica con el siguiente acrónimo PDCA, teniendo como enfoque una mejora continua

Figura 1. Ciclo de Deming

Fuente: https://www.beetrack.com/es/blog/ciclo-de-deming-etapas-ejemplos

Planificar: Esta fase es la primera etapa donde se determina el problema, mediante técnicas como la creación de grupos de trabajo, en esta fase se establece objetivos se destinan deberes para dar una solución y alcanzar los objetivos planteados

Hacer: En esta etapa los colaboradores empiezan a trabajar para lograr los objetivos planteados mediante los cambios planificados, mediante ejercicios previos, teniendo en cuenta que el equipo debe estar supervisado y realizar un piloto de prueba teniendo en cuenta la verificación y aplicación de las correcciones que se planificaron registrando lo elaborado y los resultados que se obtuvieron

Controlar: Luego de un periodo de tiempo previamente definido desde el comienzo que se realizó las actividades se inicia la evaluación de los resultados para cada objetivo planteado, de este estudio se constata la eficacia y eficiencia de las actividades realizadas, se verifica si la mejora ejecutada alcanzo el objetivo a través de herramientas de control designadas.

Actuar: En esta última fase se debe adecuar el plan de mejora, se adopta decisiones con base en el aprendizaje obtenido, se da una normalización para la solución al problema estableciendo las condiciones para mantenerlo, si en la prueba piloto se llega alcanzar el objetivo planteado, si se ha alcanzado el objetivo planteado en la prueba piloto, se establecerá el formato definitivo.

Si el objetivo planteado no se alcanzó se analizará el desarrollo para revelar los errores e iniciar un nuevo ciclo PDCA y de esta manera se cierra el ciclo retroalimentándose y de esta manera volver a la primera fase.

2.1.3. Principios

El conservar la confidencialidad, integridad y disponibilidad de la información es el objetivo del Sistema de Gestión de Seguridad de la Información.

Figura 2. Principios del SGSI

Fuente: https://www.beetrack.com/es/blog/ciclo-de-deming-etapas-ejemplos

Confidencialidad: os usuarios autorizados son los únicos con acceso al sistema ya que este se encuentra limitado, evitando que la información la cual se encuentra clasificada intencionalmente sea revelada a alguien que no tiene acceso a esta información, el mal uso del acceso a los usuarios puede conllevar a la perdida de la información.

Integridad: los usuarios autorizados son los únicos que pueden modificar o borrar la información, la información tiene que mantenerse integra y correcta sin ser manipulada por un tercero.

Disponibilidad: tienen acceso a la información solo los usuarios autorizados en un tiempo razonable, en esencia la información está disponible en el momento que se la requiere o se le necesite.

Lo fundamental de un SGSI es el diseño, implantación y mantenimiento de una serie de reglas o normativas para tramitar eficiente y eficazmente el acceso a la información, en busca de garantizar la confidencialidad, integridad y disponibilidad de la información reduciendo al mínimo la inseguridad de esta.

2.1.4. Proceso para la gestión del riesgo de la seguridad de la información

Las actividades, el procedimiento y la estimación de los riesgos en el desarrollo de la gestión del riesgo de la seguridad de la información es iterativo e incrementa el detalle y la profundidad del diagnóstico en cada una de las iteraciones, suministrando un efectivo equilibrio entre el esfuerzo requerido y la reducción del tiempo para de esta manera localiza las vulnerabilidades y de esta manera garantizar la valoración de una forma acertada los riesgos de alto impacto.

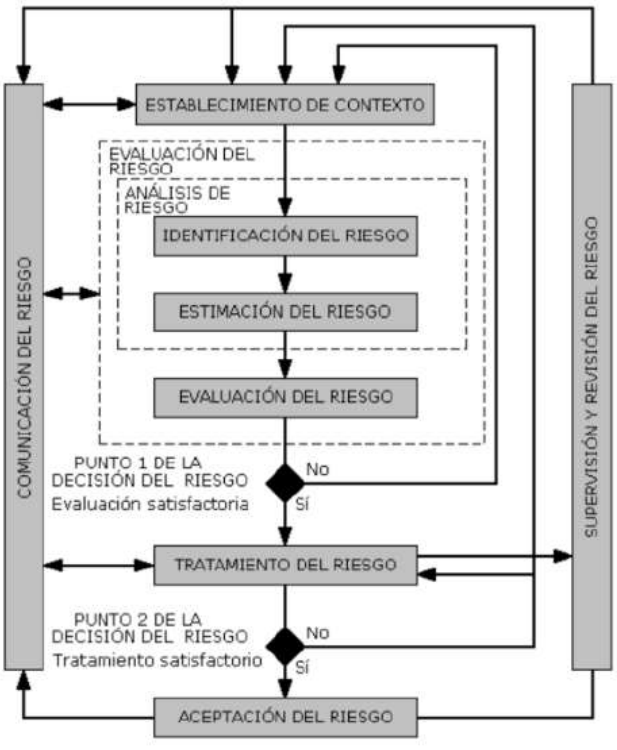
Actividades a realizarse para la gestión del riesgo de la seguridad de la información:

- Establecer el contexto
- Valorar el riesgo
- Tratar el riesgo
- Aceptar el riesgo
- Comunicar el riesgo
- Monitorear y revisar el riesgo

PROCESO PARA LA GESTIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN	
ACTIVIDADES	**PASO**
Establecimiento del contexto	**1** *Consideraciones Generales - Levantamiento de información inicial* **2** *Establecer criterios básicos para la Gestión del Riesgo* **3** *Definir alcance y límites de la Gestión del Riesgo* **4** *Establecer una organización para la operación del SGRSI*
Valoración del Riesgo	**5** *Identificar Activos de Información* **6** *Identificar las amenazas y las vulnerabilidades* **7** *Identificar los controles existentes* **8** *Identificar consecuencias* **9** *Valorar las consecuencias* **10** *Valorar los incidentes* **11** *Determinar el nivel de estimación del riesgo* **12** *Evaluar el riesgo*
Tratamiento del Riesgo	**13** *Seleccionar controles*
Aceptación del Riesgo	**14** *Aceptar el riesgo*
Comunicación del Riesgo	**15** *Comunicar el riesgo*
Monitoreo y Revisión del Riesgo	**16** *Monitorear y revisar los riesgos*

Figura 3. Proceso para la gestión del riesgo de seguridad de la información

Fuente: ISO27005



F

Figura 4. Proceso de gestión del riesgo en la seguridad de la información

Fuente: ISO27005

2.1.4.1. Establecimiento del contexto

"Se debe establecer el contexto para la gestión del riesgo de la seguridad de la información, lo cual implica establecer los criterios básicos que son necesarios para la gestión del riesgo de la seguridad de la información: definir el alcance y los límites, establecer una organización adecuada que opere la gestión del riesgo de la seguridad de la información". (GRSI., 2020)

FUENTE: GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN ABRIL 2020 GRSI.

2.1.4.2. Criterios básicos

En base a los objetivos de la gestión del riesgo y el alcance de la misma, se pueden emplear distintos enfoques. Para cada una de las iteraciones el enfoque igualmente podría ser distinto.

Es adecuado elegir o perfeccionar un enfoque apropiado que encare los criterios básicos para la gestión del riesgo, entre los criterios a considerar tenemos los criterios de: identificación, evaluación, impacto, y aceptación, concretamente.

Identificación del riesgo

Se aconseja tener en cuenta todos los activos de información que tengan una estimación de impacto elevado para proceder con el desarrollo de la evaluación del riesgo en la empresa o entidad pública.

Evaluación del riesgo

Para la evaluación del riesgo se aconseja crear parámetros con la intención de definir el riesgo existente para la seguridad de la información en la empresa o entidad pública.

Impacto del riesgo

Se aconseja crear parámetros de impacto del riesgo para poder determinar la situación del daño o de los costos para la empresa o entidad pública, ocasionados debido a un incidente de seguridad de la información.

Aceptación del riesgo

Se aconseja crear y determinar parámetros para aceptar el riesgo. Estos parámetros obedecen habitualmente de las metas, objetivos y políticas de una empresa o institución y cada una de las partes involucradas.

Las empresas o entidades públicas tienen la potestad de permitirse fijar sus escalas propias para cada grado de riesgo que se acepta o se permite según sus normativas y reglamentos internos.

Alcance y límites

Es imprescindible fijar el alcance y los limites en el desarrollo de la gestión del riesgo de la seguridad de la información, teniendo como finalidad asegurar a cada uno de los activos sobresalientes se contemplen en la estimación del riesgo. Adicionalmente, es indispensable reconocer los límites para afrontar todos y cada uno de los riesgos que se pueden descubrir al fijar estos límites.

2.2. Descripción de la propuesta

En base a los objetivos propuestos se creará una política para la gestión de seguridad de la información para una empresa de Telecomunicaciones que cumplirá con las normas vigentes resguardando toda la información ante cualquier amenaza interna o externa cumpliendo los parámetros de confidencialidad, integridad y disponibilidad de la información y emplearla en aquellos activos comprometidos de la empresa o institución

2.3. FASE I: FASE INICIAL

2.3.1. Recopilación de información

Población y Muestra

La información se recopilo por medio de encuestas realizadas a los colaboradores administrativos y colaboradores técnicos de una empresa de Telecomunicaciones.

Muestra

La empresa de telecomunicaciones actualmente cuenta con 67 colaboradores a los cuales se les realizó las encuestas, de las mismas se obtuvo 20 respuestas.

Resultados de las encuestas

Una vez realizada las encuestas se procedió a la recopilación de los datos obteniendo los siguientes resultados:

Pregunta Nro. 1

¿Realiza copias de seguridad periódicamente?

Si

No

Tabla 1.

Políticas Copias de seguridad

Colaboradores administrativos y colaboradores técnicos de una empresa de telecomunicaciones		
Variable	Frecuencia	Porcentaje
Si	7	35 %
No	13	65 %

Fuente: Elaboración propia

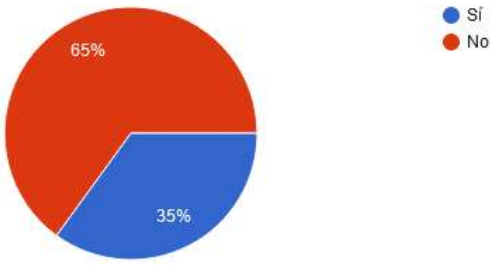


Figura 5: Copias de seguridad

Fuente: Elaboración propia

Interpretación

Los colaboradores de la empresa de Telecomunicaciones, no tienen claro la importancia o por qué se debe realizar copias de la información de una manera rutinaria o periódica.

Pregunta Nro. 2

¿Aplica políticas de seguridad de la información?

Si

No

No lo sé

Tabla 2.

Políticas de seguridad de la información

Colaboradores administrativos y colaboradores técnicos de una empresa de telecomunicaciones		
Variable	Frecuencia	Porcentaje
Si	9	45 %
No	10	50 %
No lo sé	1	5 %

Fuente: Elaboración propia

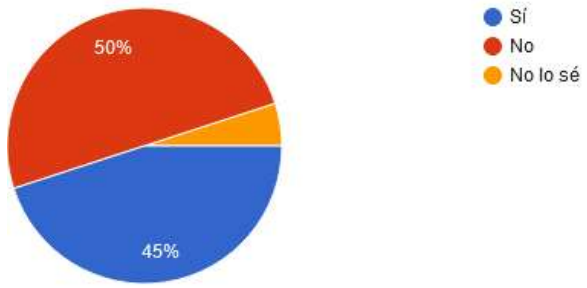


Figura 6: Políticas de seguridad de la información

Fuente: Elaboración propia

Interpretación

Los colaboradores la empresa de Telecomunicaciones, no tienen definida y/o no tienen clara una metodología o política de seguridad de la información en el uso de las tecnologías o aplicaciones actuales que a diario las ejecutan.

Pregunta Nro. 3

¿Cree que toda su información está segura y disponible 24/7?

Si

No

No lo sé

Tabla 3.

Información segura

Colaboradores administrativos y colaboradores técnicos de una empresa de telecomunicaciones		
Variable	Frecuencia	Porcentaje
Si	5	25 %
No	14	70 %
No lo sé	1	5 %

Fuente: Elaboración propia

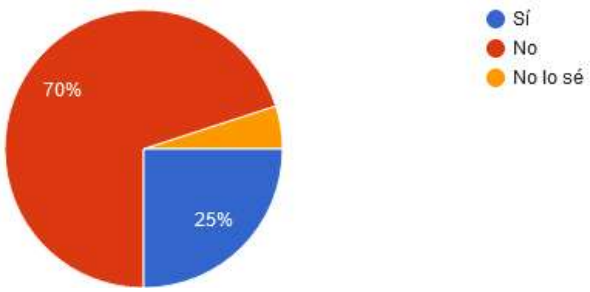


Figura 7: Información segura

Fuente: Elaboración propia

Interpretación

Los colaboradores la empresa de Telecomunicaciones, no sienten que su información se encuentre segura, sienten que la empresa no protege la integridad de sus datos, no tienen una privacidad y disponibilidad las 24 horas al día, 7 días a la semana su información la cual se aloja en los sistemas informáticos de la empresa.

2.4. Fase II. DEFINICIÓN

2.4.1. Análisis

2.4.1.1. Situación Actual

En la actualidad la empresa de telecomunicaciones se encuentra distribuida en tres localidades las cuales han sufrido cambios tanto en su equipamiento físico como tecnológico, con la implementación de nuevos equipos informáticos e instalación de nuevas aplicaciones.

Distribución actual área técnica

Planta baja - edificio administrativo

En la planta baja del edificio administrativo y considerando el crecimiento se tiene 21 puestos de trabajo, 6 equipo WI-FI de los cuales 4 son para los colaboradores de la empresa y 2 para el personal invitado, un equipo para el registro de ingreso y salida de los colaboradores y 3 cámaras para la vigilancia interna de la empresa.

Tabla 4.

Esquema actual Planta baja- edificio administrativo

DESCRIPCIÓN	CANTIDAD
BIOMÉTRICO	1
CÁMARAS	3
RED WIRELESS (ACCESS POINT)	6
DATOS, VoIP	21
TOTAL	**31**

Fuente: Elaboración Edward Illescas, Jaime Caiza, Leyla Barahona

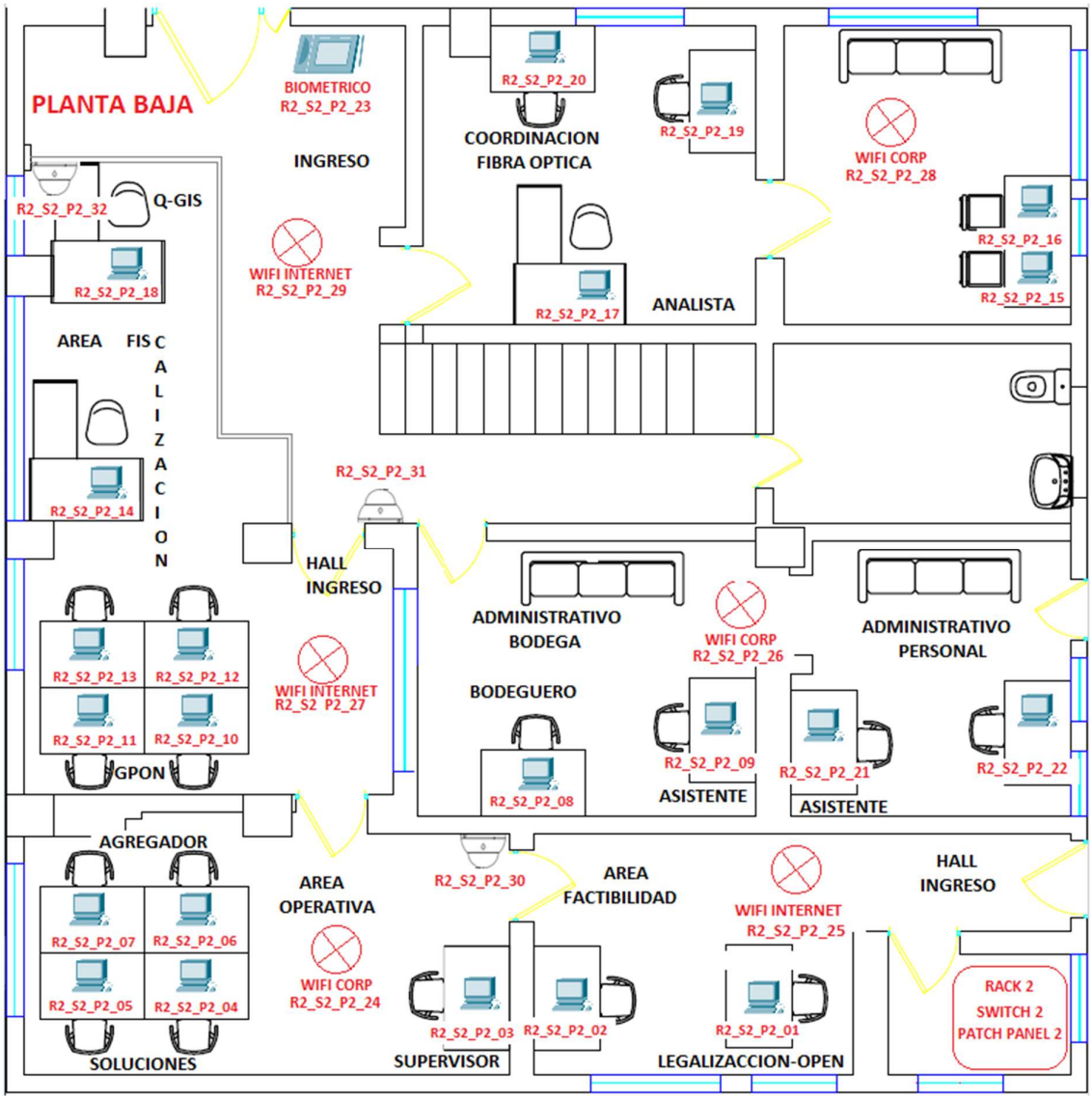


Figura 8. Esquema actual Planta baja- edificio administrativo

Fuente: Elaboración Edward Illescas, Jaime Caiza, Leyla Barahona

Primer piso - edificio administrativo

En el primer piso del edificio administrativo y considerando el crecimiento se tiene 28 puestos de trabajo, 4 equipo WI-FI de los cuales 2 son para los colaboradores de la empresa y 2 para el personal invitado, 2 impresoras y 5 cámaras para la vigilancia interna de la empresa.

Tabla 5.

Distribución Primer piso - edificio administrativo

DESCRIPCIÓN	CANTIDAD
IMPRESORAS	2
CÁMARAS	5
RED WIRELESS (ACCESS POINT)	4
DATOS, VoIP	28
TOTAL	**39**

Fuente: Elaboración**:** Edward Illescas, Jaime Caiza, Leyla Barahona

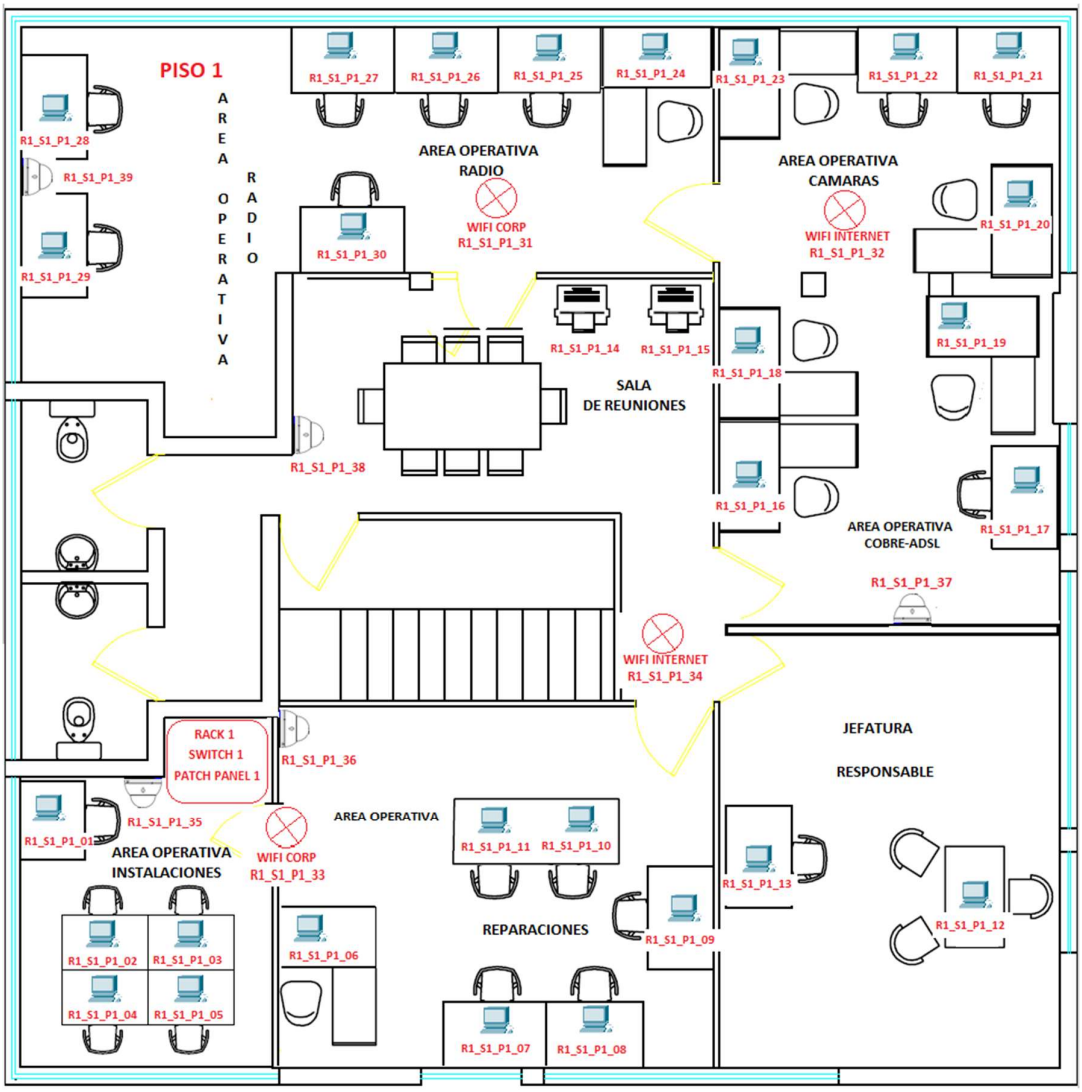


Figura 9. Esquema actual Primer piso - edificio administrativo

Fuente: Elaboración Edward Illescas, Jaime Caiza, Leyla Barahona

Planta baja - edificio área técnica

En la planta baja del edificio área técnica y considerando el crecimiento se tiene 18 puestos de trabajo, 2 equipo WI-FI para los colaboradores de la empresa, 1 impresora y 1 cámaras para la vigilancia interna de la empresa.

Tabla 6.

Distribución Planta baja - edificio área técnica

DESCRIPCIÓN	CANTIDAD
IMPRESORAS	1
CÁMARAS	1
RED WIRELESS (ACCESS POINT)	2
DATOS, VoIP	18
TOTAL	**22**

Fuente: Elaboración Edward Illescas, Jaime Caiza, Leyla Barahona

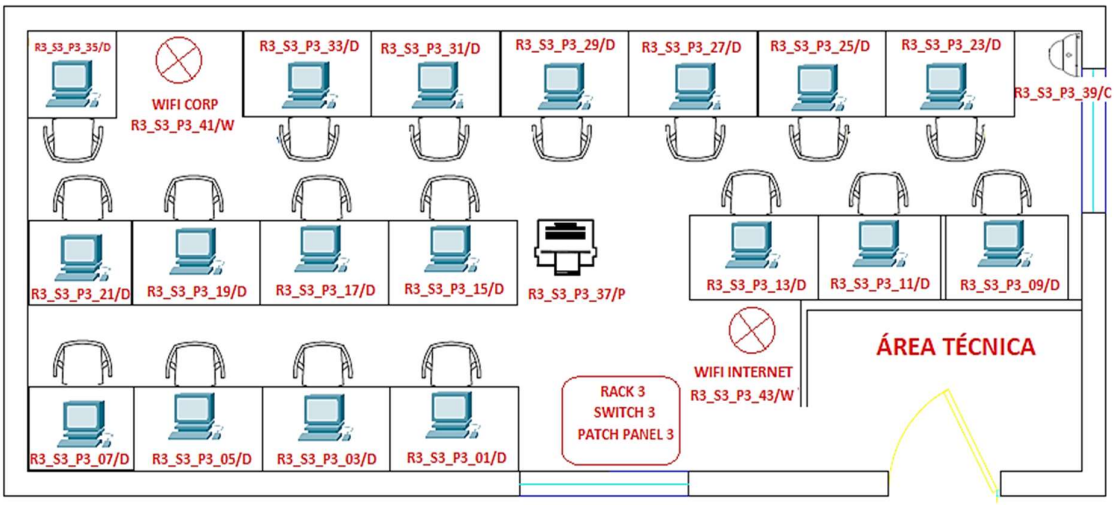


Figura 10. Esquema actual Planta baja - edificio área técnica

Fuente: Elaboración Edward Illescas, Jaime Caiza, Leyla Barahona

En esta empresa de telecomunicaciones claramente se visualiza la falta de seguridad en la información acorde a los cambios tecnológicos efectuados en la misma y mucho menos se ha considerado el crecimiento de los usuarios con acceso a la información en los últimos años.

La existencia de vulnerabilidades de la información se denota en la siguiente tabla:

Tabla 7.

Activos identificados - edificios área técnica

Nombre de Activo
Computador
Impresora
Red de datos
Access Point
Cámara de seguridad
Cortafuego
Biométrico
Router de acceso principal
Router de acceso secundario
Antivirus
Aplicaciones
Servicio de correo Exchange
Colaboradores administrativos
Colaboradores técnicos

Fuente: Elaboración propia

Por esta situación actual es necesario la creación de una política de seguridad de la información para poder disminuir las vulnerabilidades encontradas en esta empresa de Telecomunicaciones.

2.5. Fase III. EJECUCION

2.5.1. Desarrollo

En la actualidad para las empresas e instituciones públicas es de suma importancia instaurar una política de seguridad de la Información fundamentada en normativas vigentes, por medio de este documento se orientara la actuación de los colaboradores y personal contratista sobre la información procesada o generada por la empresa, de la misma manera esta política permitirá que la empresa labore cumpliendo las normativas de seguridad de la información y de este modo se ajuste con todos los requerimientos que está obligada a ejecutar la empresa o institución.

2.5.1.1. Gestión del riesgo de la seguridad de la información

Para el desarrollo de la gestión de riesgo de cada uno de los activos de la empresa o institución y la posterior creación de la política de seguridad de la información fundamentada en la metodología descrita y en base a las normativas de Seguridad de la información vigente, se define el siguiente diagrama de flujo:

Diagrama de flujo

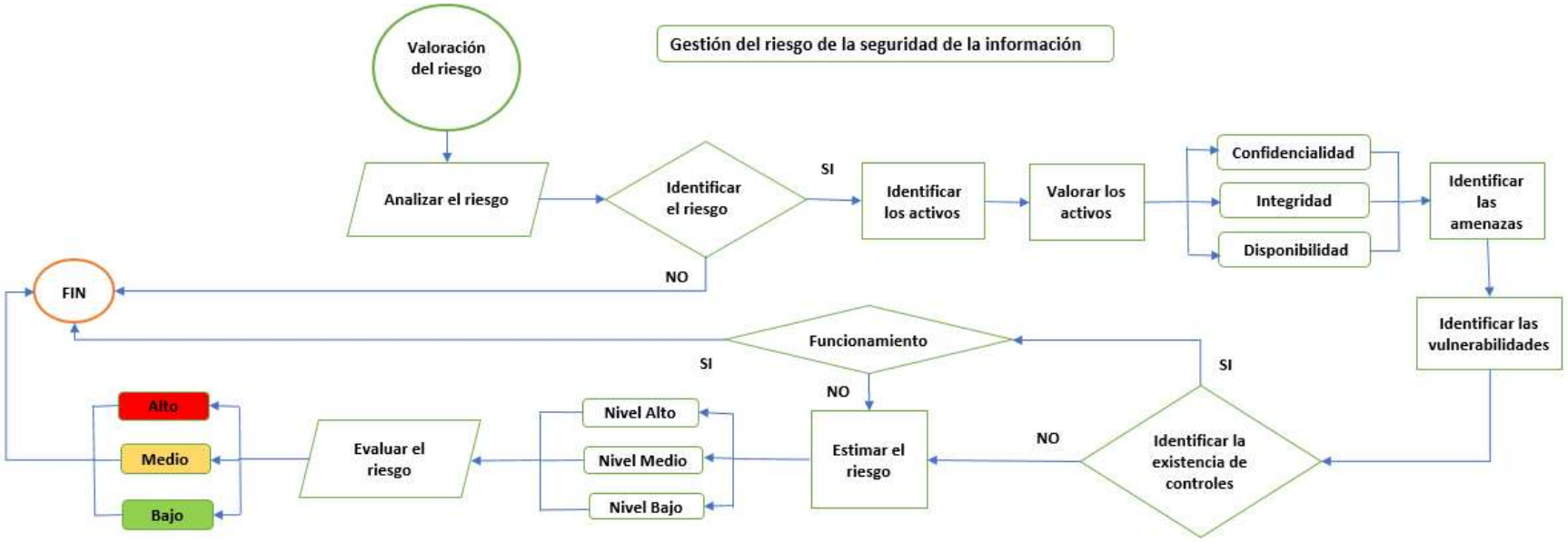


Figura 11. *G*estión del riesgo de la seguridad de la información

Fuente: Elaboración propia

2.5.1.2. Valoración del riesgo

Un riesgo es una posibilidad o exposición a que una amenaza que se presenta después de ocurrido un evento inesperado se transforme en una tragedia no deseada.

La estimación de este riesgo valora o especifica cualitativamente el riesgo y de esta manera facilita a los dueños de los activos primar los riesgos conforme a su magnitud observada o criterios fijados para ser reducidos o manejados y tomar las respectivas medidas de seguridad.

Actividades:

- Analizar el riesgo
    - Identificar el riesgo
    - Estimar el riesgo
- Evaluar el riesgo

Analizar el riesgo

Identificar el riesgo

En este punto se establece todo lo que pudiera ocasionar pérdidas para la empresa o institución, para identificar los riesgos se conforma una serie de actividades las cuales las desarrollamos a continuación:

- Identificar los activos
    - Valorar los activos
- Identificar las amenazas
- Identificar las vulnerabilidades
- Identificar la existencia de controles.

Identificar los activos

El bien que una empresa posee se denomina activo el cual puede convertirse en dinero o intercambiarse con otro bien de igual valor.

Por lo expuesto anteriormente un activo necesita de seguridad y protección. Para identificar los activos se aconseja tomar en cuenta que la información está constituida de más componentes o elementos no sólo software y hardware.

Se debe determinar al usuario de cada uno de los activos de la empresa pública o institución, el cual puede o no tener derechos sobre la propiedad del activo, pero posee la responsabilidad sobre el uso y seguridad, según competa, este colaborador es la persona idónea para evaluar los activos que tiene la empresa pública o institución

De lo antes dicho se origina un listado de activos y su debida importancia que serán sujetos a gestión del riesgo

Para la evaluación de estos activos, la institución reconocerá en primer lugar los activos a detalle los cuales de una manera general se pueden diversificar en activos primarios y activos de soporte

Primarios:

- Actividades y desarrollo del negocio.
- Información.

De soporte:

- Hardware.
- Redes.
- Software.
- Localidad
- Colaboradores.

Tabla 8.

Identificación de los activos

IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN						
Activo	**Proceso**	**Macro Subproceso**	**Tipo de Activo**	**Nombre de Activo**	**Descripción del activo**	**Ubicación**
A1	**Tecnologías de la Información y Comunicaciones**	Infraestructura	Hardware	Computador	Acceso a la red LAN en la empresa de Telecomunicaciones	**Edificio Área técnica** **Edificio administrativo** - Planta baja - Primer piso Á**rea técnica** - Planta baja
A2			Hardware	Impresora	Acceso a la red LAN en la empresa de Telecomunicaciones	**Edificio Área técnica** **Edificio administrativo** - Primer piso Á**rea técnica** - Planta baja
A3			Hardware	Red de Datos	Da Acceso a los activos de la empresa de Telecomunicaciones	**Edificio Área técnica** **Edificio administrativo** - Planta baja - Primer piso Á**rea técnica** - Planta baja
A4			Hardware	Access Point	Acceso a la red WLAN en la empresa de Telecomunicaciones	**Edificio Área técnica** **Edificio administrativo** - Planta baja - Primer piso Á**rea técnica** - Planta baja

A5		Hardware	Cámara de seguridad	Acceso de los circuitos cerrados de vigilancia en toda la empresa de Telecomunicaciones	**Edificio Área técnica** **Edificio administrativo** - Planta baja - Primer piso Á**rea técnica** - Planta baja
A6		Hardware	Cortafuego	Seguridad, permisos y control de accesos a la red LAN en toda la empresa de Telecomunicaciones	**Edificio Área técnica** **Edificio administrativo** **Rack de equipos** - Planta baja - Primer piso Á**rea técnica** **Rack de equipos** - Planta baja
A7		Hardware	Biométrico	Registro de los colaboradores	**Edificio Área técnica** **Edificio administrativo** - Planta baja
A8		Redes	Router de acceso principal	Procesamiento de trafico de la red LAN para la distribución de datos e internet	**Edificio Área técnica** **Edificio administrativo** **Rack de equipos** - Primer piso
A9	Redes y comunicaciones	Redes	Router de acceso secundario	Procesamiento del tráfico de la red de acceso a cada piso del edificio	**Edificio Área técnica** **Edificio administrativo** **Rack de equipos** - Planta baja - Primer piso Á**rea técnica** **Rack de equipos** - Planta baja
A10		Software	Antivirus	Software de seguridad	**Computadores** **Edificio Área técnica** **Edificio administrativo** - Planta baja - Primer piso Á**rea técnica** - Planta baja
A11	Aplicaciones informáticas	Software	Aplicaciones	Software para la ejecución de las gestiones	**Computadores** **Edificio Área técnica** **Edificio administrativo** - Planta baja - Primer piso Á**rea técnica** - Planta baja
A12		Software	Servicio de correo Exchange	Buzones de correo electrónico de la empresa de Telecomunicaciones	**Computadores** **Edificio Área técnica** **Edificio administrativo** - Planta baja - Primer piso Á**rea técnica** - Planta baja

A13	Talento Humano	Personal	Personal administrativo	Coordinadores de Soporte Técnico	**Edificio Área técnica** **Edificio administrativo** - Planta baja - Primer piso Á**rea técnica** - Planta baja
A14		Personal	Personal técnico	Colaboradores de Soporte Técnico	**Edificio Área técnica** **Edificio administrativo** - Planta baja - Primer piso Á**rea técnica** - Planta baja

Fuente: Elaboración propia

2.5.1.3. Valorar los activos

Es la fase en donde intervienen todos los involucrados en el negocio a fin de establecer en expresiones cualitativas la gravedad de todos los activos involucrados.

Esta valoración será elaborada en expresiones de confidencialidad, integridad y disponibilidad "alta, media o baja" donde se señala una valoración cuantitativa a cada expresión cualitativa.

A continuación, se detallan las valoraciones según los distintos criterios de la empresa en cuestiones de confidencialidad, integridad y disponibilidad de la información.

Tabla 9.

Valoración - confidencialidad de la información

CONFIDENCIALIDAD	CRITERIOS
Alta (3)	La difusión de la información que no fue autorizada la cual es confidencial o sensible conlleva un resultado desfavorable o grave para una empresa de Telecomunicaciones.
Media (2)	La difusión de la información de uso interno que no fue autorizada conlleva una consecuencia reducida para una empresa de Telecomunicaciones.
Baja (1)	La difusión de la información que es de carácter publica no conlleva ninguna consecuencia para una empresa de Telecomunicaciones.

Fuente: Elaboración propia

Tabla 10.

Valoración - Integridad de la información

INTEGRIDAD	CRITERIOS
Alta (3)	El cambio o la eliminación de la información la cual no fue autorizada conlleva un resultado desfavorable o grave para una empresa de Telecomunicaciones.
Media (2)	El cambio o la eliminación de la información la cual no fue autorizada conlleva un resultado significativo para una empresa de Telecomunicaciones.
Baja (1)	El cambio o la eliminación de la información la cual no fue autorizada conlleva un resultado insignificante para una empresa de Telecomunicaciones.

Fuente: Elaboración propia

Tabla 11.

Valoración - Disponibilidad de la información

DISPONIBILIDAD	CRITERIOS
Alta (3)	La suspensión del acceso a los sistemas informáticos o a la información, conlleva un resultado desfavorable o grave para una empresa de Telecomunicaciones.
Media (2)	La suspensión del acceso a los sistemas informáticos o a la información, conlleva un resultado significativo para una empresa de Telecomunicaciones.
Baja (1)	La suspensión del acceso a los sistemas informáticos o a la información, conlleva un resultado significativo para una empresa de Telecomunicaciones.

Fuente: Elaboración propia

DISPONIBILIDAD	CRITERIOS

Alta (3)	La suspensión del acceso a los sistemas informáticos o a la información, conlleva un resultado desfavorable o grave para una empresa de Telecomunicaciones.
Media (2)	La suspensión del acceso a los sistemas informáticos o a la información, conlleva un resultado significativo para una empresa de Telecomunicaciones.
Baja (1)	La suspensión del acceso a los sistemas informáticos o a la información, conlleva un resultado significativo para una empresa de Telecomunicaciones.

Tabla 12.

Valoración de los activos de información

VALORACIÓN DE LOS ACTIVOS DE INFORMACIÓN						
			Valoración de Impacto (pérdida)			
Nro. Activo	**Nombre de Activo**	**Tipo de soporte**	**C: Confidencialidad I: Integridad D: Disponibilidad**			
			C	**I**	**D**	**VA**
A1	Computador	Físico y Lógico	3	2	2	**2,33**
A2	Impresora	Físico y Lógico	2	1	2	**1,67**
A3	Res de datos	Físico y Lógico	2	3	3	**2,67**
A4	Access Point	Físico y Lógico	2	2	1	**1,67**
A5	Cámara de Seguridad	Físico y Lógico	2	2	3	**2,33**
A6	Cortafuego	Físico y Lógico	3	3	3	**3,00**
A7	Biométrico	Físico y Lógico	3	2	1	**2,00**
A8	Router de acceso principal	Físico y Lógico	3	3	2	**2,67**
A9	Router de acceso secundario	Físico y Lógico	2	2	1	**1,67**
A10	Antivirus	Lógico	3	2	2	**2,33**
A11	Aplicaciones	Lógico	2	2	1	**1,67**
A12	Servicio de correo Exchange	Lógico	2	2	1	**1,67**
A13	Colaborador administrativo	Lógico	1	1	1	**1,00**
A14	Colaborador técnico	Lógico	1	1	1	**1,00**

Fuente: Elaboración propia

(VA), la valoración de un activo esta dado por la media de las valoraciones de la confidencialidad, integridad y disponibilidad de la información:

$$VA = \frac{C + I + D}{3}$$

Identificación de Amenazas

Se tiene que identificar las amenazas y las razones o causas que la originaron ya que tiene la facultad de ocasionar daños graves e irreversibles a todos y cada uno de los activos de información de las empresas o instituciones.

Algunas de las amenazas consiguen dañar no solo a un activo si no a varios de ellos. Por tal motivo consiguen causar impactos diferentes dependiendo del activo o los activos que se fueron perjudicados.

Tabla 13.

Identificación de Amenazas

ANALISIS DE RIESGOS DE LOS ACTIVOS DE INFORMACIÓN			
Subprocesos	**Activo**	**Nombre de Activo**	**Amenaza**
Infraestructura	**A1**	Computador	Ingresos no autorizados Indisponibilidad de servicios Sustracción de información
	A2	Impresora	Ingresos no autorizados Indisponibilidad de servicios
	A3	Red de datos	Indisponibilidad de servicios
	A4	Access Point	Intrusos en la red Indisponibilidad de servicios
	A5	Cámara de seguridad	Ingreso de personas no deseables Sustracción de activos
	A6	Cortafuego	Ingreso no deseado a activos críticos Indisponibilidad de servicios
	A7	Biométrico	Creación de nuevas aplicaciones o funcionalidades para el registro de los colaboradores
	A8	Router de acceso Principal	Ingreso no deseado a activos críticos Indisponibilidad de servicios
	A9	Router de acceso secundario	Ingreso no deseado a activos críticos Indisponibilidad de servicios
	A10	Antivirus	Indisponibilidad de información Indisponibilidad de servicios
	A11	Aplicaciones	indisponibilidad de servicios
	A12	Servicio de correo Exchange	sustracción de información
	A13	Colaborador administrativo	Manipulación errónea de la información
	A14	Colaborador técnico	Manipulación errónea de equipos

Fuente: Elaboración propia

Identificar las Vulnerabilidades

En este punto deben ser identificadas todas las vulnerabilidades que podrían ser aprovechadas por las amenazas y lograrían ocasionar perjuicios a los activos de la empresa o institución.

Por sí misma una vulnerabilidad no causa perjuicios a los activos, para que cause algún perjuicio se necesita que exista una amenaza activa que aproveche esta vulnerabilidad.

Una vulnerabilidad no necesitaría mente requeriría de la implementación de un control si esta no tiene una amenaza que cause algún perjuicio significativo a la empresa o institución, pero es aconsejable reconocerla y vigilarla para observar si existe algún cambio.

Cave recalcar que la implementación de un control de manera errónea, en mal funcionamiento o se utilice de una forma incorrecta se puede volver en una vulnerabilidad

Tabla 14.

Valoración - Activos de información

ANALISIS DE RIESGOS DE LOS ACTIVOS DE INFORMACIÓN				
Subprocesos	**Activo**	**Nombre de Activo**	**Amenaza**	**Vulnerabilidad**
Infraestructura	**A1**	Computador	Ingresos no autorizados	Credenciales de acceso poco seguras
			Disminución de las gestiones a realizarse	Hardware con recursos limitados
			Disminución de las gestiones a realizarse	Software desactualizado
			Sustracción de información	No hay control de dispositivos externos
	A2	Impresora	Ingresos no autorizados	Credenciales de acceso poco seguras
			Indisponibilidad de servicios	Carencia de un equipo de Backup
	A3	Red de Datos	Intermitencias en la red	Patcheo inadecuado
			Indisponibilidad de servicios	Crecimiento desordenado de la red
	A4	Access Point	Intrusos en la red	Credenciales de acceso poco seguras
			Indisponibilidad de servicios	Carencia de un equipo de Backup
	A5	Cámara de seguridad	Ingreso de personas no deseables y/o sustracción de activos	Existencia de áreas sin vigilancia
			Ingreso de personas no deseables y/o sustracción de activos	Equipos continuamente dañados

A6	Cortafuego	Ingreso no deseado a activos críticos	Por falta de recursos del equipo no se puede actualizar el firmware
		Indisponibilidad de servicios	Carencia de un equipo de Backup
A7	Biométrico	Creación de nuevas aplicaciones o funcionalidades para el registro de los colaboradores	Software base incompatible con la plataforma de desarrollo actual
A8	Router de acceso principal	Ingreso no deseado a activos críticos	Credenciales de acceso poco seguras
		Indisponibilidad de servicios	Carencia de un equipo de Backup
A9	Router de acceso secundario	Ingreso no deseado a activos críticos	Credenciales de acceso poco seguras
		Indisponibilidad de servicios	Carencia de un equipo de Backup
A10	Antivirus	Ingreso no deseado a activos críticos	Activación de filtros de seguridad
		Indisponibilidad de servicios	Actualización periódicamente
A11	Aplicaciones	indisponibilidad de servicios	Software desactualizado
A12	Servicio de correo Exchange	sustracción de información	Activación de filtros de seguridad
A13	Colaborador administrativo	indisponibilidad de servicios	Falta de capacitación
A14	Colaborador técnico	indisponibilidad de servicios	Falta de capacitación

Fuente: Elaboración propia

Identificación de Existencia de Controles

En este punto identificaremos todos y cada uno de los controles existentes en la empresa o institución y con ello evitar la duplicidad de controles existente, y a su vez se puede verificar que los controles ya implementados estén siendo aplicados correctamente dado que si el control existente no está funcionando de una forma adecuada puede ser causa de una vulnerabilidad y causar daño a un activo.

Tabla 15.

Valoración de los activos de información

ANALISIS DE RIESGOS DE LOS ACTIVOS DE INFORMACIÓN					EVALUACIÓN DE RIESGOS
Subprocesos	**Activo**	**Nombre de Activo**	**Amenaza**	**Vulnerabilidad**	**Controles implementados existentes**
Infraestructura	**A1**	Computador	Ingresos no autorizados	Credenciales de acceso poco seguras	Soporte local

		Disminución de las gestiones a realizarse	Hardware con recursos limitados	Ninguno
		Disminución de las gestiones a realizarse	Software desactualizado	Ninguno
		Sustracción de información	Control de dispositivos externos	Ninguno
A2	Impresora	Ingresos no autorizados	Credenciales de acceso poco seguras	Soporte externo
		Indisponibilidad de servicios	Carencia de un equipo de Backup	Ninguno
A3	Red de Datos	Intermitencias en la red	Patcheo de la red	Mantenimiento local
		Indisponibilidad de servicios	Crecimiento de la red	Ninguno
A4	Access Point	Intrusos en la red	Credenciales de acceso poco seguras	Mantenimiento local
		Indisponibilidad de servicios	Carencia de un equipo de Backup	Ninguno
A5	Cámara de seguridad	Ingreso de personas no deseables y/o Sustracción de activos	Existencia de áreas sin vigilancia	Ninguno
		Ingreso de personas no deseables y/o Sustracción de activos	Equipos continuamente dañados	Ninguno
A6	Cortafuego	Ingreso no deseado a activos críticos	Por falta de recursos del equipo no se puede actualizar el firmware	Ninguno
		Indisponibilidad de servicios	Carencia de un equipo de Backup	Ninguno
A7	Biométrico	Creación de nuevas aplicaciones o funcionalidades para el registro de los colaboradores	Software base incompatible con la plataforma de desarrollo actual	Ninguno
A8	Router de acceso principal	Ingreso no deseado a activos críticos	Credenciales de acceso poco seguras	Mantenimiento local
		Indisponibilidad de servicios	Carencia de un equipo de Backup	Ninguno
A9	Router de acceso secundario	Ingreso no deseado a activos críticos	Credenciales de acceso poco seguras	Mantenimiento local
		Indisponibilidad de servicios	Carencia de un equipo de Backup	Ninguno
A10	Antivirus	Ingreso no deseado a activos críticos	Activación de filtros de seguridad	Soporte externo
		Indisponibilidad de servicios	Actualización periódicamente	Soporte externo
A11	Aplicaciones	indisponibilidad de servicios	Software desactualizado	Soporte externo
A12	Servicio de correo Exchange	sustracción de información	Activación de filtros de seguridad	Soporte externo
A13	Colaborador administrativo	indisponibilidad de servicios	Capacitación	Ninguno

	A14	Colaborador técnico	indisponibilidad de servicios	Capacitación	Ninguno

Fuente: Elaboración propia

Estimación o Análisis del riesgo

Posteriormente a la identificación de los riesgos se procede a la utilización de una metodología para el análisis de riesgos, el método a ser utilizado es el método cuantitativo o cualitativo y de esta manera logar la cuantificación de todos y cada uno de los riesgos identificados, para esta ponderación se utilizará una escala que nos permita calificar los atributos y observar las dimensiones potenciales de estos riesgos y sus posibles consecuencias a los activos de la empresa o institución.

Evaluación del riesgo

Para la evaluación del riesgo compararemos la estimación de los riesgos versus los criterios ponderados para la evaluación y aceptación de los riesgos determinados en el ámbito que estamos desarrollando, y de esta manera establecer la relevancia del riesgo el cual es presentado en forma numérica fundamentado en la valoración que se dé a los activos de información, la relevancia de las amenazas y la repercusión de las vulnerabilidades

Criterios de probabilidad de ocurrencia de amenazas

A continuación, puntualizaremos valores calificativos y numéricos que se utilizaran para dar valor a la probabilidad de una amenaza que podría desembocar en una de las vulnerabilidades ya existentes.

Tabla 16.

Valoración de los activos de información

Nivel de amenazas	Criterio por probabilidad	Criterio por condición de ocurrencia	Criterio por activo
Alto (3)	La ocurrencia es muy probable (probabilidad > 50%)	Bajo circunstancias normales	El atacante se beneficia en gran medida por el ataque, tiene la capacidad técnica para ejecutarlo y la vulnerabilidad es fácilmente explotable
Medio (2)	La ocurrencia es probable (probabilidad =50%)	Por errores descuidos	El atacante se beneficia de alguna manera por el ataque, tiene la capacidad técnica para

			ejecutarlo y la vulnerabilidad es fácilmente explotable
Bajo (1)	La ocurrencia es menos probable (probabilidad >0 y <50%)	en rara ocasión	El atacante no se beneficia del ataque

Fuente: Gestión de riesgos de seguridad de la información abril 2020 GRSI

Nivel de vulnerabilidad según el criterio de probabilidad:

Tabla 17.

Valoración de los activos de información

NIVEL DE VULNERABILIDAD	CRITERIO
Alto (3)	No existe ninguna medida de seguridad implementada para prevenir la ocurrencia de la amenaza
Medio (2)	Existen medidas de seguridad implementadas que no reducen la probabilidad de ocurrencia de la amenaza a un nivel aceptable
Bajo (1)	La medida de seguridad es adecuada

Fuente: Gestión de riesgos de seguridad de la información abril 2020 GRSI

Criterio de la Evaluación de Riesgos

El nivel de riesgo de cada uno de los activos está dado por la Valoración de los activos multiplicado por el nivel de amenaza y el nivel de vulnerabilidad de la información.

Nivel de riesgo = Valoración del activo ∗ Nivel de amenaza ∗ Nivel de vulnerabilidad

Tabla 18.

Nivel de criterio de vulnerabilidad

NIVEL DE VULNERABILIDAD	CRITERIO
1 - 3	**Riesgo Bajo**
4 - 8	**Riesgo Medio**
9 - 27	**Riesgo Alto**

Fuente: Elaboración propia

Tabla 19.

Valoración de los activos de información

ANÁLISIS DE RIESGOS					IMPACTO	PROBABILIDAD		EVALUACIÓN DE RIESGOS		
SUBPROCESOS	**Nro. Activo**	**Nombre Activo**	**Amenaza**	**Vulnerabilidad**	**CID**	**Nivel de Amenaza**	**Nivel de vulnerabilidad**	**controles implementados existentes**	**cálculo de estimación del Riesgo**	**Nivel del riesgo**
			Ingresos no autorizados	Credenciales de acceso poco seguras	2,33	3	1	Soporte local	7	EL RIESGO ES MEDIO
			Disminución de las gestiones a realizarse	Hardware con recursos limitados	2,33	1	1	Ninguno	2,3	EL RIESGO ES BAJO
Infraestructura	**A1**	Computador	Disminución de las gestiones a realizarse	Software desactualizado	2,33	1	1	Ninguno	2,3	EL RIESGO ES BAJO
			Sustracción de información	Control de dispositivos externos	2,33	3	3	Ninguno	21,0	EL RIESGO ES ALTO
			Perdida de la información	No existe Backup de la información	2,33	3	3	Ninguno	21,0	EL RIESGO ES ALTO
Infraestructura	**A2**	Impresora	Disminución de las gestiones a realizarse	Credenciales de acceso poco seguras	1,67	1	1	Soporte local	1,7	EL RIESGO ES BAJO
			Indisponibilidad de servicios	Carencia de un equipo de Backup	1,67	1	1	Ninguno	1,7	EL RIESGO ES BAJO
Infraestructura	**A3**	Red de Datos	Intermitencias en la red	Patcheo de la red	2,67	2	3	Mantenimiento local	16,0	EL RIESGO ES ALTO
			Indisponibilidad de servicios	Crecimiento de la red	2,67	2	3	Ninguno	16,0	EL RIESGO ES ALTO
Infraestructura	**A4**	AP	Intrusos en la red	Credenciales de acceso poco seguras	1,67	2	2	Mantenimiento local	6,7	EL RIESGO ES MEDIO

			Indisponibilidad de servicios	Carencia de un equipo de Backup	1,67	3	3	Ninguno	15,0	EL RIESGO ES ALTO
Infraestructura	**A5**	Cámara de seguridad	Ingreso de personas no deseables y/o sustracción de activos	Existencia de áreas sin vigilancia	2,33	3	3	Ninguno	21,0	EL RIESGO ES ALTO
			Ingreso de personas no deseables y/o sustracción de activos	Equipos continuamente dañados	2,33	3	1	Ninguno	7,0	EL RIESGO ES MEDIO
Infraestructura	**A6**	Cortafuego	Ingreso no deseado a activos críticos	Por falta de recursos del equipo no se puede actualizar el firmware	3,00	3	2	Ninguno	18,0	EL RIESGO ES ALTO
			Indisponibilidad de servicios	Carencia de un equipo de Backup	3,00	3	3	Ninguno	27,0	EL RIESGO ES ALTO
Infraestructura	**A7**	Biométrico	Creación de nuevas aplicaciones o funcionalidades para el registro de los colaboradores	Software base incompatible con la plataforma de desarrollo actual	2,00	1	1	Ninguno	2,0	EL RIESGO ES BAJO
Infraestructura	**A8**	Router de acceso Principal	Ingreso no deseado a activos críticos	Credenciales de acceso poco seguras	2,67	2	1	Mantenimiento local	5,3	EL RIESGO ES MEDIO
			Indisponibilidad de servicios	Carencia de un equipo de Backup	1,67	2	3	Ninguno	10,0	EL RIESGO ES ALTO
Infraestructura	**A9**	Router de acceso secundario	Ingreso no deseado a activos críticos	Credenciales de acceso poco seguras	1,67	2	1	Mantenimiento local	3,3	EL RIESGO ES MEDIO
			Indisponibilidad de servicios	Carencia de un equipo de Backup	2,33	2	3	Ninguno	14,0	EL RIESGO ES ALTO
Infraestructura	**A10**	Antivirus	Ingreso no deseado a activos críticos	Activación de filtros de seguridad	2,33	3	1	Soporte local	7,0	EL RIESGO ES MEDIO

			Indisponibilidad de servicios	Actualización periódicamente	1,67	3	1	Soporte local	5,0	EL RIESGO ES MEDIO
Infraestructura	**A11**	Aplicaciones	indisponibilidad de servicios	Software desactualizado	1,67	2	1	Soporte local	3,3	EL RIESGO ES MEDIO
Infraestructura	**A12**	Servicio de correo Exchange	sustracción de información	Activación de filtros de seguridad	1,67	2	1	Soporte local	3,3	EL RIESGO ES MEDIO
Personal	**A13**	Colaborador administrativo	indisponibilidad de servicios	Capacitación	1,00	2	3	Ninguno	6,0	EL RIESGO ES MEDIO
Personal	**A14**	Colaborador técnico	indisponibilidad de servicios	Capacitación	1,00	2	3	Ninguno	6,0	EL RIESGO ES MEDIO

Fuente: Elaboración propia

2.5.1.4. Tratamiento del Riesgo

Para el desarrollo del tratamiento de los riesgos de cada uno de los activos de la empresa o institución y la posterior creación de la política de seguridad de la información fundamentada en la metodología descrita y en base a las normativas vigentes, se define el siguiente diagrama de flujo:

Diagrama de flujo

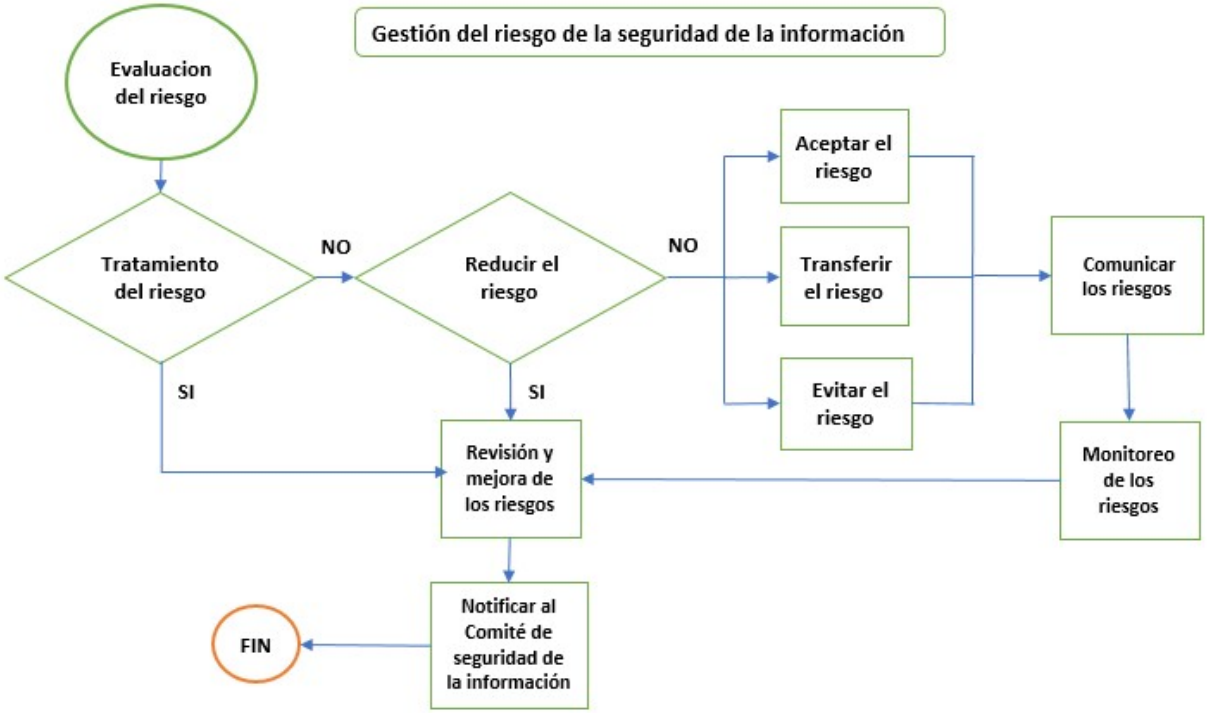


Figura 12. Tratamiento del Riesgo

Fuente: Elaboración propia

Para el tratamiento del riesgo es necesario que adoptemos decisiones entorno a los riesgos existentes en concordancia con las estrategias que plantea la empresa o institución.

Tenemos que elegir cuáles serán los controles que se implementarán en cada activo de la información para evitar, reducir, aceptar o transferir el riesgo y determinar el plan para tratarlo.

Las alternativas de control para tratar el riesgo se elegirán fundamentándonos en los resultados de la estimación del riesgo tomando en cuenta el costo y beneficio deseado para poder poner en práctica estas alternativas.

Si con un costo considerablemente bajo se logra reducir riesgos altos, se tendría que aplicar esas alternativas de control, por otro lado, si las alternativas de control adicionales no son económicamente bajas se necesitara un estudio para señalar si se justifica o no ponerlas en práctica.

Tratamiento del riesgo:

- Reducir el riesgo
- Aceptar el riesgo
- Evitar el riesgo
- Transferir el riesgo

Reducir el riesgo

Por medio de las alternativas de control se debe reducir el riesgo de modo que al volver a evaluar el riesgo resulte bajo, seleccionando alternativas adecuadas y justificadas que cumplan los requerimientos necesarios.

Debemos tomar en consideración los criterios de aceptación del riesgo sin dejar de lado tanto los requerimientos legales como los contractuales, así como también se debe contemplar los costos y tiempo para la implementación de las alternativas de control al igual que los aspectos técnicos, ambientales y culturales.

En general al elegir alternativas de control adecuadas se puede disminuir el nivel de riesgo de seguridad de la información a bajo costo de implementación.

Aceptación del riesgo

La aceptación del riesgo se debe tomar con conocimiento y objetividad cumpliendo las políticas y criterios de la empresa o institución.

Si el valor de la implementación de un control de seguridad rebasa el costo de un activo de información que se va a proteger o es bajo el nivel de riesgo, se tomará la determinación de aceptar los riesgos con

sus respectivas responsabilidades de esta decisión llevando un registro de la misma de una manera oficial.

Transferir el riesgo

La transferencia del riesgo consiste en trasladar el riesgo a otra localidad para poderlo administrar de una forma más adecuada teniendo en cuenta la valoración del mismo.

Evitar el riesgo

Si para el tratamiento de los riesgos el costo es considerablemente alto y excede los beneficios o a su vez los riesgos que se identifiquen sean muy altos, se podría tomar la decisión de evitar este riesgo, a través del retiro de dicha actividad o cambiando las circunstancias en las cuales se desarrolla la misma.

Comunicar los riesgos

Esta actividad es muy importante ya que con la comunicación del riesgo se tomará una decisión de cuál será el procedimiento para gestionar los riesgos al compartir o cambiar la información acerca de estos.

Es de suma importancia la comunicación efectiva de las partes comprometidas ya que la resolución que se tomen podría causar un efecto relevante, con la comunicación garantizamos que los encargados de la implementación de la gestión de riesgo y los encargados de los activos de información entiendan los fundamentos por los cuales se está tomando esta resolución y porque se necesitan implantar estas medidas.

Monitoreo de los riesgos

Tomando en cuenta que los riesgos pueden cambiar drásticamente de un momento a otro o en otras palabras los riesgos son variables, por ende, las amenazas, vulnerabilidades y los resultados cambian de la misma manera, por este motivo, la necesidad de contar con un monitoreo eficaz que nos asegure con la detención de estos cambios y lograr un control efectivo de las amenazas sobre los activos de información, este procedimiento se lo debe repetir periódicamente y con mucha regularidad.

Revisión y mejora

La revisión constante nos garantiza que se está cumpliendo con la valoración del riesgo y de la misma manera su tratamiento debe continuar siendo eficaz y apropiado en la actualidad, todas estas observaciones y revisiones, así como las mejoras que se podrían estimar se deben notificar al Comité de seguridad de la información y de esta manera tener la seguridad de que se tomaran las mejores decisiones respecto a estas mejoras y tener la destreza de solventar las mismas.

2.6. Fase IV. Política

2.6.1. POLÍTICA DE SEGURIDAD

La creación de una política de seguridad de la información fundamentada en las normativas y estándares internacionales de buenas prácticas, nos ayudara a proteger, resguardar y prevenir amenazas a los datos e información generada en una empresa de Telecomunicaciones.

2.6.2. Objetivo

Crear una política de seguridad de la información en base a normas que encaminaran a un adecuado uso de la tecnología actual implementada en una empresa de Telecomunicaciones y de esta manera garantizar la disponibilidad, confidencialidad e integridad de la información de una manera continua.

2.6.3. Alcance

La Política que se describirá en el presente documento será aplicable a todos los colaboradores de una empresa de Telecomunicaciones y personal externo con su debida autorización previa para el uso de los activos de información.

2.6.4. Responsabilidades

Destinar el área responsable que implemente, actualice y vigile el cumplimiento de la política de seguridad de la información creada para una empresa de Telecomunicaciones.

Se conformará un comité de seguridad de la información el cual estará constituido por los responsables de todas las áreas de la empresa quienes entre otras responsabilidades tienen que:

- Gestionar la aprobación de la política de seguridad de la información y normas institucionales en materia de seguridad de la información, por parte de la máxima autoridad de la Institución.
- Realizar el seguimiento de los cambios significativos de los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
- Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad de la información, con nivel de impacto alto.
- Coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios, en base a la gestión de seguridad de la información vigente.
- Promover la difusión de la seguridad de la información dentro de la institución.
- Coordinar el proceso de gestión de la continuidad de la operación de los servicios y sistemas de información de la institución frente a incidentes de seguridad imprevistos.

Dentro de esta área se designará un oficial de seguridad de la Información el cual debe tener conocimiento en Seguridad de la Información y Gestión de Proyectos, quien será el responsable de

coordinar las acciones requeridas para dar cabal cumplimiento a la política de seguridad de la información

2.6.5. Procedimientos

Seguidamente, se detalla todos y cada uno de los procedimientos que se tendrán que ejecutar para garantizar la disponibilidad, confidencialidad e integridad de la información.

2.6.5.1. Política para el computador

Objetivo. Garantizar el acceso seguro y el correcto funcionamiento del computador para asegurar el óptimo desempeño de las gestiones asignadas a diario.

Alcance. La política actual aplica a todos los computadores instalados en una empresa de Telecomunicaciones.

Política: Es de obligatoriedad identificar al propietario o usuario del activo, fijar las responsabilidades y la correcta operatividad del mismo, evitar la sustracción de información por medio de accesos de dispositivos externos, y de esta manera, garantizar el óptimo desempeño de las gestiones que se realizan a diario afianzando la disponibilidad, confidencialidad e integridad de la información.

Responsabilidad del usuario del activo

- El usuario tiene la responsabilidad de establecer una credencial de acceso seguro con una mezcla de números, letras mayúsculas, minúsculas y caracteres especiales, modificándola con frecuencia.
- El usuario tiene total responsabilidad sobre el acceso de dispositivos externos para la gestión del uso de la información.

Controles.

Se deben considerar los siguientes controles.

- Las credenciales de acceso deben ser seguras
- Los recursos de Hardware no deben ser limitados
- Los recursos de Software deben ser actualizados con frecuencia
- Se debe autorizar el acceso de dispositivos externos

Restricciones y prohibiciones.

Está completamente prohibido:

- Usar el activo para labores ajenas a las gestiones asignadas por la empresa

- Manipular el activo de forma inadecuada a nivel hardware y software
- Trasladar el activo a un lugar no autorizado y mucho menos al exterior del edificio

2.6.5.2. Política de la Impresora

Objetivo. Garantizar el acceso seguro, el correcto funcionamiento y la disponibilidad de la impresora 24 horas al día, 7 días a la semana para asegurar el óptimo desempeño de las gestiones asignadas a diario.

Alcance. La política actual aplica a todos las impresoras instaladas en una empresa de Telecomunicaciones.

Política: Es de obligatoriedad identificar al propietario o usuario del activo, fijar las responsabilidades, la correcta operatividad del mismo, contar con una impresora de respaldo para realizar la reposición cuando deje de funcionar por cualquier eventualidad y de esta manera, garantizar el óptimo desempeño de las gestiones que se realizan a diario afianzando la disponibilidad, confidencialidad e integridad de la información.

Responsabilidad del usuario del activo.

- El usuario tiene la responsabilidad de establecer una credencial de acceso seguro con una mezcla de números, letras mayúsculas, minúsculas y caracteres especiales, modificándola con frecuencia.
- El usuario tiene total responsabilidad sobre la correcta operatividad y usos del activo.

Controles.

Se deben considerar los siguientes controles.

- Las credenciales de acceso deben ser seguras
- La existencia de una impresora para reposición

Restricciones y prohibiciones.

Está completamente prohibido:

- Usar el activo para labores ajenas a las gestiones asignadas por la empresa
- Manipular el activo de forma inadecuada
- Trasladar el activo a un lugar no autorizado y mucho menos al exterior del edificio

2.6.5.3. Política para la red de datos

Objetivo. Garantizar el correcto funcionamiento de la red de datos para asegurar el óptimo desempeño de las gestiones asignadas a diario.

Alcance. La política actual aplica a toda la red LAN de una empresa de Telecomunicaciones**.**

Política: Es de obligatoriedad identificar al usuario encargado del activo, fijar las responsabilidades y la correcta operatividad del mismo, y de esta manera, garantizar el óptimo desempeño de las gestiones que se realizan a diario afianzando la disponibilidad, confidencialidad e integridad de la información.

Responsabilidades.

Los usuarios del activo tienen las siguientes responsabilidades:

- Mantener en buen estado la conectividad física de la red de datos.
- Atender el crecimiento de la red de datos por incremento de usuarios.

Controles.

Se deben considerar los siguientes controles.

- El cableado utilizado en la red debe estar en óptimas condiciones
- La existencia de cable para la reposición por deterioro y/o crecimiento de la red

Restricciones y prohibiciones.

Está completamente prohibido:

- Usar el activo para labores ajenas a las gestiones asignadas por la empresa
- Manipular el activo de forma inadecuada

2.6.5.4. Política para el Access Point

Objetivo. Garantizar el correcto funcionamiento de los equipos Access Point para asegurar el óptimo desempeño de las gestiones asignadas a diario.

Alcance. La política actual aplica a todos los equipos Access Point instalados en una empresa de Telecomunicaciones**.**

Política: Es de obligatoriedad identificar al usuario encargado del activo, y del mismo modo identificar a los usuarios que tendrán el acceso a la red inalámbrica, fijar las responsabilidades y la correcta operatividad de los mismos, y de esta manera, garantizar el óptimo desempeño de las gestiones que se realizan a diario afianzando la disponibilidad, confidencialidad e integridad de la información.

Responsabilidades.

Los encargados del activo tienen las siguientes responsabilidades:

- Mantener operativa la disponibilidad de la conexión inalámbrica 24 horas al día, 7 días a la semana.

- Establecer credenciales de acceso seguras con una mezcla de números, letras mayúsculas, minúsculas y caracteres especiales, modificándolas con frecuencia.

Controles.

Se deben considerar los siguientes controles.

- Las credenciales de acceso inalámbrico deben ser seguras
- La existencia de equipos para la reposición por deterioro o daño.

Restricciones y prohibiciones.

Está completamente prohibido:

- Revelar o compartir las credenciales de acceso a la red inalámbrica a usuarios no autorizados para el uso de la misma
- Usar el acceso inalámbrico para labores ajenas a las gestiones asignadas por la empresa
- Manipular el activo de forma inadecuada
- Trasladar el activo a un lugar no autorizado y mucho menos al exterior del edificio

2.6.5.5. Política para la Cámara de seguridad

Objetivo. Garantizar el correcto funcionamiento de la cámara de seguridad para evitar o evidenciar la sustracción de activos de la empresa.

Alcance. La política actual aplica a todos las cámaras de seguridad instaladas en una empresa de Telecomunicaciones**.**

Política: Es de obligatoriedad identificar al usuario encargado del activo y fijar las responsabilidades y la correcta operatividad de los mismos, y de esta manera, garantizar la disponibilidad, confidencialidad e integridad de la información.

Responsabilidades.

Los encargados del activo tienen las siguientes responsabilidades:

- Mantener operativa la disponibilidad de las cámaras de seguridad 24 horas al día, 7 días a la semana.
- Monitorear el ingreso de usuarios no autorizados a la empresa y comunicar de los acontecimientos a los encargados de la seguridad.
- Monitorear y/o identificar la sustracción de activos de la empresa y comunicar de los acontecimientos a los encargados de la seguridad.

Controles.

Se deben considerar los siguientes controles.

- Que no existan áreas no vigiladas y/o no monitoreadas
- La existencia de equipos para la reposición por deterioro o daño.

Restricciones y prohibiciones.

Está completamente prohibido:

- Revelar o compartir las credenciales de acceso a las cámaras de seguridad a usuarios no autorizados para el uso de la misma
- Usar el acceso a las cámaras de seguridad para labores ajenas a las gestiones asignadas por la empresa
- Manipular el activo de forma inadecuada
- Trasladar el activo a un lugar no autorizado y mucho menos al exterior del edificio

2.6.5.6. Política para el Cortafuego

Objetivo. Garantizar el correcto funcionamiento del cortafuego para evitar el ingreso de usuarios no autorizados a la red de datos de la empresa y de esta manera, garantizar el óptimo desempeño de las gestiones que se realizan a diario afianzando la disponibilidad, confidencialidad e integridad de la información.

Alcance. La política actual aplica al cortafuegos instalado en la red de datos en una empresa de Telecomunicaciones**.**

Política: Es de obligatoriedad identificar al usuario encargado del activo y fijar las responsabilidades y la correcta operatividad del mismo, y de esta manera, garantizar la disponibilidad, confidencialidad e integridad de la información.

Responsabilidades.

Los encargados del activo tienen las siguientes responsabilidades:

- Mantener operativa la disponibilidad del cortafuego las 24 horas al día, 7 días a la semana.
- Establecer credenciales de acceso seguras con una mezcla de números, letras mayúsculas, minúsculas y caracteres especiales, modificándolas con frecuencia.

Controles.

Se deben considerar los siguientes controles.

- Que el firmware del equipo este siempre actualizado
- La existencia de otro equipo para la reposición por deterioro o daño.

Restricciones y prohibiciones.

Está completamente prohibido:

- Revelar o compartir las credenciales de acceso al Cortafuegos a usuarios no autorizados
- Usar el acceso al Cortafuegos para labores ajenas a las gestiones asignadas por la empresa
- Manipular el activo de forma inadecuada
- Trasladar el activo a un lugar no autorizado y mucho menos al exterior del edificio

2.6.5.7. Política para el Biométrico

Objetivo. Garantizar el correcto funcionamiento del Biométrico para garantizar el registro del ingreso y salida de los colaboradores de la empresa garantizando el control de asistencia diaria y de esta manera afianzar la disponibilidad, confidencialidad e integridad de la información.

Alcance. La política actual aplica al biométrico instalado en la red de datos en una empresa de Telecomunicaciones**.**

Política: Es de obligatoriedad identificar al usuario encargado del activo y fijar las responsabilidades y la correcta operatividad del mismo, y de esta manera, garantizar la disponibilidad, confidencialidad e integridad de la información.

Responsabilidades.

Los encargados del activo tienen las siguientes responsabilidades:

- Mantener operativa la disponibilidad del Biométrico las 24 horas al día, 7 días a la semana.

Controles.

Se deben considerar los siguientes controles.

- Que el firmware del equipo este siempre actualizado.

Restricciones y prohibiciones.

Está completamente prohibido:

- Usar el Activo para labores ajenas a las gestiones asignadas por la empresa
- Manipular el activo de forma inadecuada
- Trasladar el activo a un lugar no autorizado y mucho menos al exterior del edificio

2.6.5.8. Política para el Router de acceso principal

Objetivo. Garantizar el correcto funcionamiento del equipo Router de acceso principal, evitar el ingreso de usuarios no autorizados, asegurar la conectividad y administrar el tráfico de todos los dispositivos conectados a la red de datos de la empresa y de esta manera, garantizar el óptimo desempeño de las gestiones que se realizan a diario afianzando la disponibilidad, confidencialidad e integridad de la información.

Alcance. La política actual aplica al equipo Router de acceso Principal instalado en la red de datos en una empresa de Telecomunicaciones**.**

Política: Es de obligatoriedad identificar al usuario encargado del activo y fijar las responsabilidades y la correcta operatividad del mismo, y de esta manera, garantizar la disponibilidad, confidencialidad e integridad de la información.

Responsabilidades.

Los encargados del activo tienen las siguientes responsabilidades:

- Mantener operativa la disponibilidad del equipo Router de acceso Principal las 24 horas al día, 7 días a la semana.
- Establecer credenciales de acceso seguras con una mezcla de números, letras mayúsculas, minúsculas y caracteres especiales, modificándolas con frecuencia.

Controles.

Se deben considerar los siguientes controles.

- Las credenciales de acceso deben ser seguras
- Que el firmware del equipo este siempre actualizado
- Que todos los dispositivos conectados a la red estén autorizados
- La correcta administración del tráfico de la red
- La existencia de otro equipo para la reposición por deterioro o daño.

Restricciones y prohibiciones.

Está completamente prohibido:

- Revelar o compartir las credenciales de acceso al equipo Router de acceso a usuarios no autorizados
- Usar el equipo Router de accesos para labores ajenas a las gestiones asignadas por la empresa
- Manipular el activo de forma inadecuada
- Trasladar el activo a un lugar no autorizado y mucho menos al exterior del edificio

2.6.5.9. Política para el Router de acceso secundario

Objetivo. Garantizar el correcto funcionamiento del equipo Router de acceso secundario, evitar el ingreso de usuarios no autorizados, asegurar la conectividad y administrar el tráfico de todos los dispositivos conectados a la red de datos de la empresa de Telecomunicaciones y de esta manera, garantizar el óptimo desempeño de las gestiones que se realizan a diario afianzando la disponibilidad, confidencialidad e integridad de la información.

Alcance. La política actual aplica al equipo Router de acceso secundario instalado en la red de datos en una empresa de Telecomunicaciones**.**

Política: Es de obligatoriedad identificar al usuario encargado del activo y fijar las responsabilidades y la correcta operatividad del mismo, y de esta manera, garantizar la disponibilidad, confidencialidad e integridad de la información.

Responsabilidades.

Los encargados del activo tienen las siguientes responsabilidades:

- Mantener operativa la disponibilidad del equipo Router de acceso Secundario las 24 horas al día, 7 días a la semana.
- Establecer credenciales de acceso seguras con una mezcla de números, letras mayúsculas, minúsculas y caracteres especiales, modificándolas con frecuencia.

Controles.

Se deben considerar los siguientes controles.

- Las credenciales de acceso deben ser seguras
- Que el firmware del equipo este siempre actualizado
- Que todos los dispositivos conectados a la red estén autorizados
- La correcta administración del tráfico de la red
- La existencia de otro equipo para la reposición por deterioro o daño.

Restricciones y prohibiciones.

Está completamente prohibido:

- Revelar o compartir las credenciales de acceso al equipo Router de acceso a usuarios no autorizados
- Usar el equipo Router de accesos para labores ajenas a las gestiones asignadas por la empresa
- Manipular el activo de forma inadecuada
- Trasladar el activo a un lugar no autorizado y mucho menos al exterior del edificio

2.6.5.10. Política para el Antivirus

Objetivo. Garantizar el correcto funcionamiento del Antivirus para evitar el ingreso de amenazas a la red de datos de la empresa y de esta manera, garantizar el óptimo desempeño de las gestiones que se realizan a diario afianzando la disponibilidad, confidencialidad e integridad de la información.

Alcance. La política actual aplica al Antivirus instalado en la red de datos en una empresa de Telecomunicaciones**.**

Política: Es de obligatoriedad identificar al usuario encargado del activo y fijar las responsabilidades y la correcta operatividad del mismo, y de esta manera, garantizar la disponibilidad, confidencialidad e integridad de la información.

Responsabilidades.

Los encargados del activo tienen las siguientes responsabilidades:

- Mantener operativa la disponibilidad del Antivirus las 24 horas al día, 7 días a la semana.

Controles.

Se deben considerar los siguientes controles:

- Que el Antivirus este instalado en todos los computadores de la empresa de Telecomunicaciones
- Que el Antivirus este siempre actualizado
- Que el licenciamiento para uso del antivirus no este vencido.

Restricciones y prohibiciones.

Está completamente prohibido:

- Desinstalar el Antivirus del computador

2.6.5.11. Política para las Aplicaciones

Objetivo. Garantizar el correcto funcionamiento de las Aplicaciones instaladas en el computador y de esta manera asegurar el óptimo desempeño de las gestiones que se realizan a diario, afianzando la disponibilidad, confidencialidad e integridad de la información.

Alcance. La política actual aplica a las Aplicaciones instaladas en los computadores existentes en una empresa de Telecomunicaciones**.**

Política: Es de obligatoriedad identificar al usuario encargado del activo y fijar las responsabilidades y la correcta operatividad del mismo, y de esta manera, garantizar la disponibilidad, confidencialidad e integridad de la información.

Responsabilidades.

Los encargados del activo tienen las siguientes responsabilidades:

- Mantener operativa la disponibilidad de las Aplicaciones las 24 horas al día, 7 días a la semana.

Controles.

Se deben considerar los siguientes controles:

- Que las Aplicaciones estén instaladas en todos los computadores de la empresa de Telecomunicaciones
- Que las Aplicaciones este siempre actualizadas
- Que el licenciamiento para uso de las Aplicaciones no este vencido.

Restricciones y prohibiciones.

Está completamente prohibido:

- Desinstalar las Aplicaciones del computador
- Usar las Aplicaciones para labores ajenas a las gestiones asignadas por la empresa d Telecomunicaciones

2.6.5.12. Política para el Servicio de correo Exchange

Objetivo. Garantizar el correcto funcionamiento del Servicio de correo Exchange instalado en el computador y de esta manera asegurar el óptimo desempeño de las gestiones que se realizan a diario, afianzando la disponibilidad, confidencialidad e integridad de la información.

Alcance. La política actual aplica al Servicio de correo Exchange instalado en los computadores existentes en una empresa de Telecomunicaciones**.**

Política: Es de obligatoriedad identificar al usuario encargado del activo y fijar las responsabilidades y la correcta operatividad del mismo, y de esta manera, garantizar la disponibilidad, confidencialidad e integridad de la información.

Responsabilidades.

Los encargados del activo tienen las siguientes responsabilidades:

- Mantener operativa la disponibilidad del Servicio de correo Exchange las 24 horas al día, 7 días a la semana.

Controles.

Se deben considerar los siguientes controles:

- Que el Servicio de correo Exchange esté instalado en todos los computadores de la empresa
- Que el licenciamiento para uso del Servicio de correo Exchange no este vencido.

Restricciones y prohibiciones.

Está completamente prohibido:

- Desinstalar el del Servicio de correo Exchange del computador
- Usar el Servicio de correo Exchange para labores ajenas a las gestiones asignadas por la empresa

- Propagar mensajes con información no autorizada de la empresa de Telecomunicaciones

2.6.5.13. Política para el Colaborador administrativo

Objetivo. Garantizar el correcto desempeño del Colaborador administrativo y de esta manera asegurar el óptimo cumplimiento de las gestiones que se realizan a diario, afianzando la disponibilidad, confidencialidad e integridad de la información.

Alcance. La política actual aplica a los Colaboradores administrativos que laboran en una empresa de Telecomunicaciones**.**

Política: Es de obligatoriedad identificar a todos los Colaboradores administrativos, fijar las responsabilidades y actividades a ser encomendadas, y de esta manera, garantizar la disponibilidad, confidencialidad e integridad de la información.

Responsabilidades.

Los Colaboradores administrativos tienen las siguientes responsabilidades:

- Organizar las gestiones que se realizaran a diario.
- Ejecutar todas las actividades que le fueron encomendadas según su perfil de contratación

Controles.

Se deben considerar los siguientes controles:

- Que todos los colaboradores administrativos cumplan con las actividades diarias encomendadas según su perfil de contratación
- Que todos los colaboradores administrativos cumplan con la capacitación requerida

Restricciones y prohibiciones.

Está completamente prohibido:

- Que los colaboradores administrativos realicen labores ajenas a las gestiones asignadas por la empresa de Telecomunicaciones
- Que los colaboradores administrativos se ausenten de la empresa en horarios de trabajo

2.6.5.14. Política para el Colaborador técnico

Objetivo. Garantizar el correcto desempeño del Colaborador técnico y de esta manera asegurar el óptimo cumplimiento de las gestiones que se realizan a diario, afianzando la disponibilidad, confidencialidad e integridad de la información.

Alcance. La política actual aplica a los Colaboradores técnicos que laboran en una empresa de Telecomunicaciones**.**

Política: Es de obligatoriedad identificar a todos los Colaboradores técnicos, fijar las responsabilidades y actividades a ser encomendadas, y de esta manera, garantizar la disponibilidad, confidencialidad e integridad de la información.

Responsabilidades.

Los Colaboradores técnicos tienen las siguientes responsabilidades:

- Ejecutar las gestiones que se realizaran a diario.
- Ejecutar todas las actividades que le fueron encomendadas según su perfil de contratación

Controles.

Se deben considerar los siguientes controles:

- Que todos los colaboradores técnicos cumplan con las actividades diarias encomendadas según su perfil de contratación
- Que todos los colaboradores técnicos cumplan con la capacitación requerida

Restricciones y prohibiciones.

Está completamente prohibido:

- Que los colaboradores técnicos realicen labores ajenas a las gestiones asignadas por la empresa de Telecomunicaciones
- Que los colaboradores técnicos se ausenten de la empresa en horarios de trabajo

Fase V: Resultados

- Se desarrolló el marco conceptual para la gestión de riesgo de seguridad de la información, en base a las normativas de seguridad de la información vigentes, el cual fue de gran utilidad para el desarrollo de la política de seguridad de la información de una empresa de Telecomunicaciones.
- En base a la supervisión en los lugares donde se encuentran los activos de información y la encuesta realizada a los colaboradores que trabajan en la empresa de Telecomunicaciones se pudo diagnosticar las vulnerabilidades actuales de los activos de información.
- Mediante la valoración de los activos se pudo establecer el nivel de riesgo existente en los activos de la empresa de Telecomunicaciones
- Se creo una política de seguridad de la información para una empresa de telecomunicaciones que cumple con los estándares y normativas de seguridad de la información vigentes la cual ayudara a la empresa a minimizar el nivel de riesgos existentes en sus activos de información.

2.7. Matriz de articulación

En la presente matriz se sintetiza la articulación del producto realizado con los sustentos teóricos, metodológicos, estratégicos-técnicos y tecnológicos empleados.

Tabla 20.

Matriz de articulación

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	CLASIFICACIÓN TIC
Identificación de los activos de información	Estándares internacionales ISO/IEC 27001 ISO/IEC 27005	Investigación de campo	Análisis del estado actual de todos los activos de información	Descripción y ubicación de los activos de información en una empresa de Telecomunicaciones	Se identificará y ubicará los activos de información fundamentada en las normativas de seguridad de la información
Valoración de los activos de información	Estándares internacionales ISO/IEC 27001 SO/IEC 27005	Experimental	Se da una valoración a los activos de información mediante los criterios de confidencialidad, integridad y disponibilidad	Se le da un valor numérico a cada uno de los activos de información en una empresa de Telecomunicaciones	Se valorará los activos en base a los criterios de confidencialidad, integridad y disponibilidad fundamentada en las normativas de seguridad de la información
Análisis de riesgos de los activos de información	Estándares internacionales ISO/IEC 27001 ISO/IEC 27005	Experimental	Análisis de los riesgos de los activos de información en base a las amenazas y vulnerabilidades localizadas	Se detalla los riesgos de los activos de información encontrados en una empresa de Telecomunicaciones	Se evaluarán los riesgos de los activos de información encontrados en base de las amenazas y vulnerabilidades fundamentada en las normativas de seguridad de la información
Tratamiento de los riesgos de los activos de información	Estándares internacionales ISO/IEC 27001 ISO/IEC 27005	Experimental	Reducir los riesgos de los activos de información en base a aceptación, transferencia, y/o evitando el riesgo	Minimizar los riesgos de los activos de información de una empresa de Telecomunicaciones	Revisión de las mejoras y Notificar al Comité de seguridad de la información fundamentada en las normativas de seguridad de la información

Fuente: Elaboración propia

CONCLUSIONES

Se estableció el marco teórico para la gestión del riesgo de seguridad de la información de una empresa de Telecomunicaciones, en base a las normativas de seguridad de la información vigentes.

Se evaluó el riesgo para la seguridad de la información mediante el análisis, identificación y estimación del riesgo de los activos de una empresa de Telecomunicaciones.

Se describió el tratamiento de los riesgos para la seguridad de la información mediante la reducción, aceptación, transferencia y comunicación del mismo.

Se creo una política de seguridad de la información acorde a los requerimientos de una empresa de Telecomunicaciones

Con la creación de la política de la seguridad de la información para una empresa de Telecomunicaciones se garantiza la disponibilidad, confidencialidad e integridad de la información.

Con la creación de la política de la seguridad de la información para una empresa de Telecomunicaciones se garantiza la operatividad y disponibilidad de los activos de la misma, las 24 horas al día, los 7 días a la semana, y de esta manera no tener complicaciones para ejecutar las gestiones generadas diariamente en la empresa.

Con la creación de la política de seguridad de la información para una empresa de Telecomunicaciones se tiene como disposición o requerimiento la obligatoriedad de identificar a los usuarios encargados de los activos y fijar las responsabilidades y la correcta operatividad de los mismos, y de esta manera, garantizar la disponibilidad, confidencialidad e integridad de la información.

Con la creación de la política de seguridad de la información para una empresa de Telecomunicaciones se tiene como disposición o requerimiento la creación de un Comité de seguridad de la información el cual es el encargado de que esta política de seguridad de la información se cumpla en su totalidad y a su vez monitore las revisiones y mejoras, para minimizar los riesgos de los activos de información.

RECOMENDACIONES

Revisar el marco teórico para la gestión del riesgo de seguridad de la información y las normativas de seguridad de la información una vez año con la intención de mantener actualizada la política de seguridad de la información de una empresa de Telecomunicaciones.

Evaluar con frecuencia los nuevos riesgos de seguridad de la información que podrían darse en el transcurso del tiempo mediante el análisis, identificación y estimación del riesgo de los activos de una empresa de Telecomunicaciones.

Ejecutar en forma periódica el tratamiento de los riesgos para la seguridad de la información mediante la reducción, aceptación, transferencia y comunicación del mismo.

Implementar la política de seguridad de la información creada acorde a una empresa de Telecomunicaciones

Implementar la política de seguridad de la información creada para una empresa de Telecomunicaciones, para de esta manera resguardar y proteger la disponibilidad, confidencialidad e integridad de la información.

Implementar la política de seguridad de la información creada para una empresa de Telecomunicaciones, para resguardar y proteger la operatividad y disponibilidad de los activos de la misma, las 24 horas al día, los 7 días a la semana, y de esta manera no tener complicaciones para ejecutar las gestiones generadas diariamente en la empresa.

Implementar la política de seguridad de la información creada para una empresa de Telecomunicaciones, y de esta manera mantener la disposición o requerimiento de la obligatoriedad de identificar a los usuarios encargados de los activos y fijar las responsabilidades y la correcta operatividad de los mismos, y de esta manera, resguardar y proteger la disponibilidad, confidencialidad e integridad de la información.

Crear un Comité de seguridad de la información el cual será el encargado de que esta política de seguridad de la información se cumpla en su totalidad y a su vez monitore las revisiones y mejoras, para minimizar los riesgos de los activos de información.

BIBLIOGRAFÍA

Alberto, G. A. (2007). Diseño y Gestión de un Sistema de Gestión de Seguridad de Información ISO 27001:2005. Colombia: Marcombo

Briseño, E. (2020). Planificación y ejecución de evaluaciones de seguridad informática desde un enfoque de Ethical Hacking. España: Área de Innovación y Desarrollo, S.L.

Darwin, C. (1998). El origen del hombre. Madrid: Biblioteca Edaf.

Fern, V. (2012). Sistema de Gestión de Seguridad de la Información. España: Académica Española.

García, F. y Albarrán, S. (2015). Guía para Implantar un Sistema de Gestión de Seguridad de Información: Basada en la Norma ISO/IEC 27001. México: EAE

García, S. (2005). Diseño e implementación de un sistema de gestión de seguridad de la información. Universidad Politécnica de Cataluña. España

Instituto Ecuatoriano de Normalización (2012). NORMA TÉCNICA ECUATORIANA NTE INEN-ISO/IEC 27000:2012. Recuperado de https://www.normalizacion.gob.ec/buzon/normas/nte_inen_iso_iec_27000extracto.pdf

Miguel, J. (2015). Protección de Datos y Seguridad de la Información. España: RA-MA.

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2020a). Acuerdo Ministerial 025-2019. Recuperado de https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/01/Registro-Oficial-Acuerdo-Ministerial-No.-025-2019-EGSI-version-2.0.pdf

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2020b). GUÍA PARA LA IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN. Recuperado de https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/04/GU%C3%8DA-PARA-LA-IMPLEMENTACI%C3%93N-DEL-EGSI-ABRIL2020.pdf

Pagliari, G. y Eterovic, J. (2012). Metodología de Análisis de Riesgos Informáticos. España: Académica Española.

Servicio Ecuatoriano de Normalización. (2016). NTE INEN-ISO/IEC 27000 Cuarta edición 2016-11. Recuperado de https://www.normalizacion.gob.ec/buzon/normas/nte_inen_iso_iec_27000.pdf

Silva, F. E., Segadas, L. G., y Bezerra, E. K. (2014). Gestión de la seguridad de la información. Ecuador: CEDIA.

Telefónica, S.A. y Morán L. (2010). ISO/IEC 20000. Guía completa de aplicación para la gestión de los servicios de tecnologías de la información. España: AENOR.

ANEXO 1

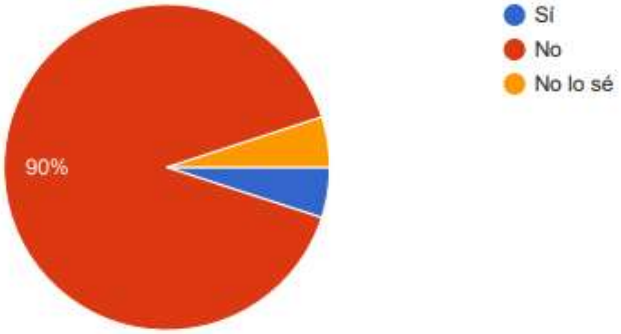
Encuestas completas con los resultados obtenidos

20 respuestas

Publicar análisis

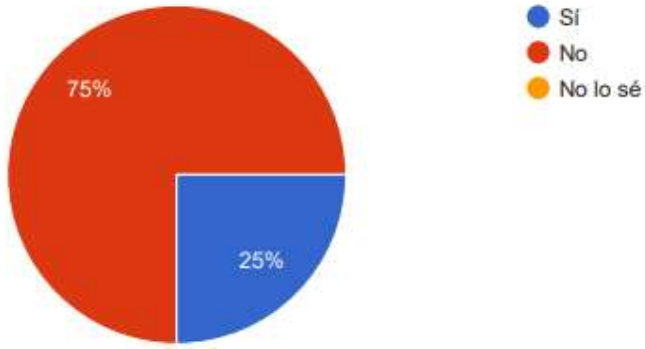
¿La red local (LAN) es adecuada?

20 respuestas



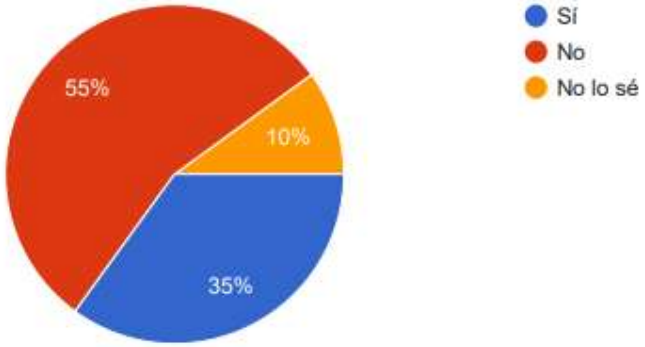
¿La red local WLAN es adecuada?

20 respuestas



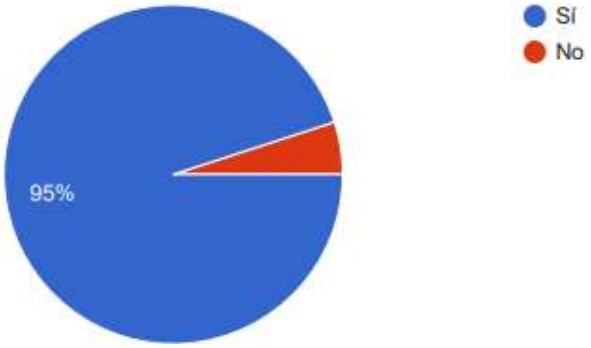
¿Utiliza Antivirus, Cortafuegos/Firewall (software o hardware)?

20 respuestas



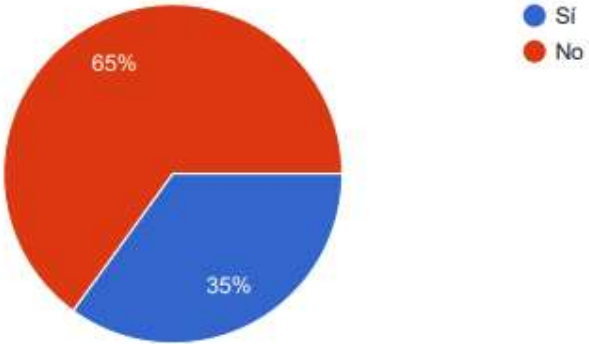
¿Usa mecanismos de autenticación para acceder a los ordenadores [nombre de usuario y contraseña] ?

20 respuestas



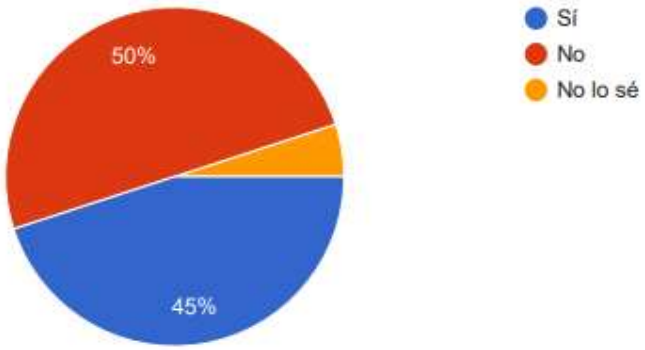
¿Realiza copias de seguridad periódicamente?

20 respuestas



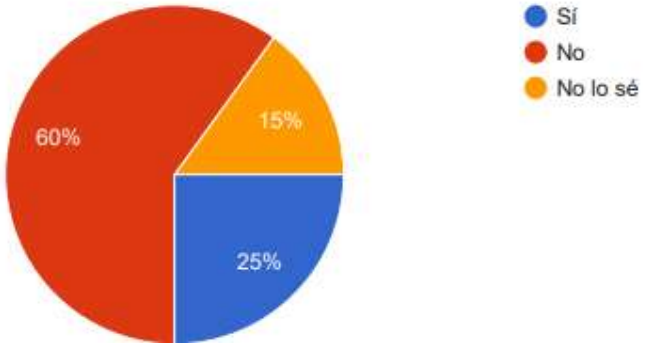
¿Aplica políticas de seguridad de la información ?

20 respuestas



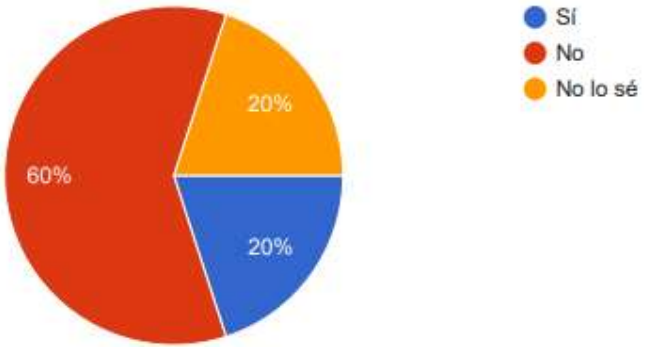
¿La red esta segmentada por el tipo de usuarios que la utilizan?

20 respuestas



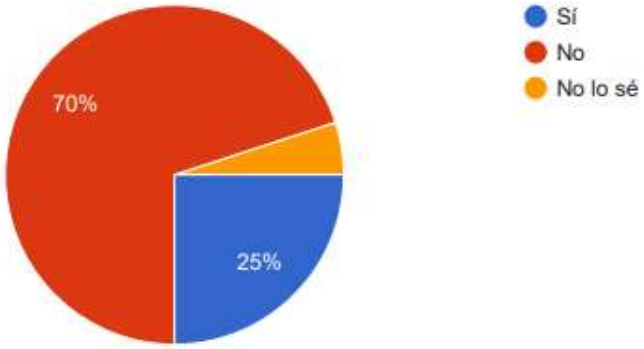
¿La infraestructura física de la red cumple con los estándares y/o normativas requeridos?

20 respuestas



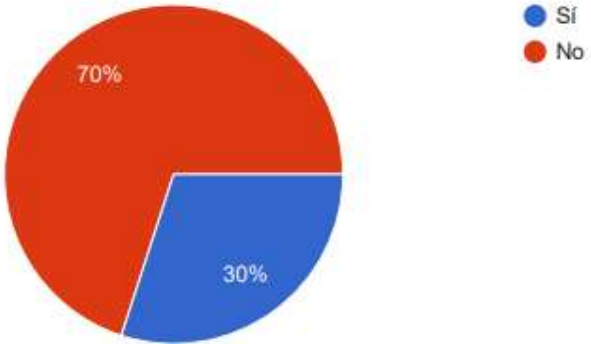
¿Cree que toda su información está segura y disponible 24/7?

20 respuestas



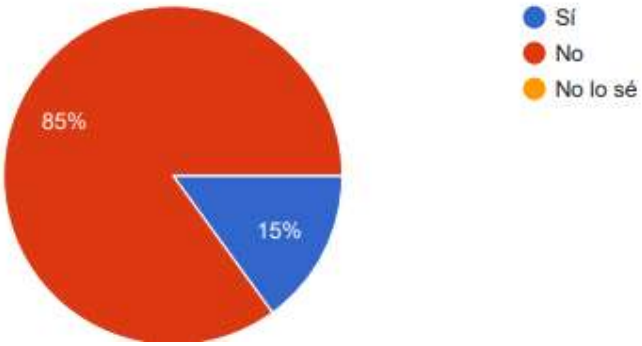
¿El ancho de banda actual es suficiente para realizar los trabajos diarios?

20 respuestas



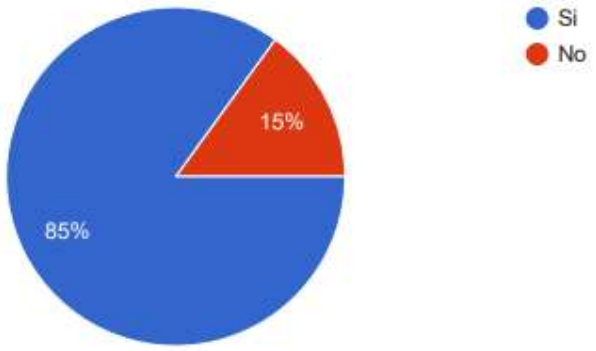
¿Su conectividad a la red es estable?

20 respuestas



¿A tenido problemas de conectividad?

20 respuestas



Agregue un comentario o recomendación

10 respuestas

Se debe implementar accesos o permisos a usuarios

UNA MODERNIZACION ACOMPAÑADA DE UN CONTINUO MONITOREO Y ACTUALIZACION DE EQUIPOS SERIA ÓPTIMO

Sería conveniente se dicten cursos de seguridad de la información presenciales

Se debe mejorar la red lan

Mejoren el servicio..

Ninguno

Monitoreo de redes mas frecuentes en horas de saturación.

Socializar sobre la seguridad de la información ya que desconozco si existe en el área que trabajamos