DISEÑO DE UN SGSI PARA EL ÁREA DE TI DE CENTRO DE CONTACTOS

GERMAN ANDRES OLANO TREJOS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA -UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SANTIAGO DE CHILE
2020

DISEÑO DE UN SGSI PARA EL ÁREA DE TI DE CENTRO DE CONTACTOS

GERMAN ANDRES OLANO TREJOS

Proyecto de grado - Proyecto aplicado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Director del Proyecto
Eduard Antonio Mantilla Torres

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SANTIAGO DE CHILE
2020

Nota de aceptación

_____

_____

_____

_____

_____

_____

_____
Firma del presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Santiago de Chile, octubre de 2020

DEDICATORIA

El trabajo realizado está dedicado para mi madre, apoyo fundamental en muchos proyectos de vida mediante sus consejos, confianza, esfuerzo y dedicación de muchos años, los cuales fueron la base para construir mi presente. A Darling, cuya confianza y apoyo me han dado fuerza para tomar decisiones de vida que antes no hubiera podido, dando real importancia a mis sueños y mis intereses en cada paso que doy. Finalmente, mis amigos, Henry y Elkin, que siempre me impulsaron a buscar un poco más allá en mi educación y me han apoyado en el camino para ser profesional.

AGRADECIMIENTOS

Este proyecto de grado ha sido un proceso en el cual se ha puesto esfuerzo y dedicación, pero que a su vez ha sido posible por el apoyo de diferentes personas que han estado presentes durante el tiempo que duró la especialización, así como el periodo que ha sido destinado para el desarrollo y aplicación del presente trabajo, personas que han aportado de diferentes maneras y a quienes, aun cuando no mencione en los siguientes párrafos, quiero agradecer por haber sido parte.

A Darling, por su confianza, por creer en mí, por enseñarme a no tener miedo a dar esos pasos que exigen valentía y coraje, que no todos están dispuestos a dar para dejar su zona de confort y buscar sueños más grandes.

A mi madre y mi familia, quienes siempre han hecho parte de mis proyectos mediante sus consejos, su apoyo y sus enseñanzas.

A Luis Ángel, Juan Carlos, Wilson, Yesid y el equipo de trabajo que me abrieron sus puertas para aplicar los conocimientos adquiridos.

CONTENIDO

GLOSARIO 13

RESUMEN 15

ABSTRACT 17

INTRODUCCIÓN 18

1 DEFINICIÓN DEL PROBLEMA 23

1.1 PRESENTACIÓN DEL TEMA 23
1.2 ANTECEDENTES 23
1.3 DESCRIPCIÓN DEL PROBLEMA 29
1.4 FORMULACIÓN DEL PROBLEMA 31
1.5 DEFINICIÓN 31
1.6 DELIMITACIÓN 31
1.7 SUBTEMAS 31
1.8 RELACIÓN CON OTRAS ÁREAS DE ESTUDIO 32
1.9 ALCANCE 32

2 JUSTIFICACIÓN 34

3 OBJETIVOS 37

3.1 OBJETIVO GENERAL 37
3.2 OBJETIVOS ESPECÍFICOS 37

4 MARCO REFERENCIAL 38

4.1 MARCO CONTEXTUAL 38
4.1.1 Descripción de la empresa. 38
4.1.2 Misión. 38
4.1.3 Visión. 38
4.1.4 Valores. 38
4.1.5 Áreas de negocio. 39
4.1.6 Organigrama 40
4.1.7 Ubicación física. 40
4.1.8 Área de TI 40
4.2 MARCO TEÓRICO 41
4.2.1 Incidentes de seguridad. 41
4.2.1.1 Software no autorizado 41
4.2.1.2 Virus\Caballo de Troya. 43
4.2.1.3 Virus informático. 44
4.2.1.4 Phishing. 44
4.2.1.6 Robo de elementos críticos de hardware. 48

4.2.1.7 Ataques de aplicaciones web – Inyección de SQL. 49
4.2.1.8 Ataque de aplicaciones web – Directory Transversal. 50
4.2.1.9 Negación del servicio. 50
4.2.2 Normas y estándares. 53
4.2.2.1 CRAM 55
4.2.2.2 COBIT 57
4.2.2.3 ITIL. 59
4.2.2.4 OCTAVE 60
4.2.2.5 MAGERIT 61
4.2.2.6 ISO 27000 62
4.2.2.7 Metodología PDCA. 65
4.3 MARCO CONCEPTUAL 67
4.3.1 Información. 67
4.3.2 Seguridad de la Información 68
4.3.3 Vulnerabilidad 68
4.3.4 Amenaza 68
4.3.5 Riesgo 68
4.3.6 Impacto 68
4.3.7 Incidente 68
4.3.8 Tratamiento del riesgo 69
4.3.9 Valoración del riesgo 69
4.3.10 Control 69
4.3.11 Política 69
4.3.12 Procedimiento 69
4.3.13 Activo 69
4.4 MARCO LEGAL 69
4.4.1 Panorama sobre la legislación de delitos informáticos 69
4.4.2 Relación de delitos y leyes colombianas sobre seguridad informática y seguridad de la información. 72
4.4.3 Ley de habeas data. 76
4.4.4 Ley de delitos informáticos. 79
5 DISEÑO METODOLÓGICO 81
5.1 METODOLOGÍA DE INVESTIGACIÓN 81
5.2 METODOLOGÍA DE DESARROLLO 82
5.3 UNIVERSO Y MUESTRA 86
6 ESTADO DE LA ORGANIZACIÓN EN SGSI 87
7 INVENTARIO DE ACTIVOS 109
7.1 VALORACIÓN DE LOS ACTIVOS EN LOS DOMINIOS 110
8 ANÁLISIS DE RIESGOS 113

8.1 AMENAZAS 113
8.2 RIESGOS 129
9 PROBLEMAS DETECTADOS 147
9.1 ANÁLISIS SEGÚN EL NIVEL DE RIESGO 147
9.1.1 Catástrofe 147
9.1.2 Desastre 148
9.1.3 Extremadamente Crítico 148
9.1.4 Muy Crítico 149
9.1.5 Crítico 149
9.1.6 Muy alto 149
9.1.7 Medio, bajo y despreciable 150
9.2 ANALISIS DE ACUERDO CON LAS AMENAZAS 150
10 SALVAGUARDAS 165
11 ROLES Y RESPONSABILIDADES 169
12 DISEÑO SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 172
12.1 ALCANCE 172
12.2 POLÍTICA GENERAL 173
12.3 POLITICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 174
12.3.1 Organización para la seguridad de la información 174
12.3.2 Personal externo 179
12.3.3 Gestión de activos 180
12.3.4 Medios removibles 185
12.3.5 Respaldo y copias de seguridad 186
12.3.6 Recursos humanos 187
12.3.7 Control de acceso 191
12.3.8 Criptografía 196
12.3.9 Instalaciones y seguridad física 198
12.3.10 Equipos informáticos 203
12.3.11 Operaciones 206
12.3.12 Gestion de cambios 208
12.3.13 Comunicaciones 210
12.3.14 Proveedores 214
12.3.15 Adquisición, desarrollo y mantenimiento de sistemas 215
12.3.16 Incidentes de seguridad 219
12.3.17 Continuidad del negocio 221
12.3.18 Cumplimiento 224
12.3.19 Gestión de los registros y auditoría 225
12.3.20 Plan de recuperación de desastres 229
12.4 FORMACIÓN 230

13 RESULTADOS 232
14 RECOMENDACIONES 236
15 CONCLUSIONES 248

LISTA DE FIGURAS

Figura 1. Evaluaciones de Seguridad....24
Figura 2. Soluciones de seguridad....25
Figura 3. Políticas de seguridad....26
Figura 4. *Frameworks* de seguridad....26
Figura 5. Obstáculos a la seguridad....27
Figura 6. Organigrama Telemarketing S.A.S....40
Figura 7. Ejemplo de ataque tipo Directory Transversal....50
Figura 8. Estándares relacionados con TI....55
Figura 10. Cumplimiento de la documentación ISO 27001....88
Figura 11. Áreas que responden la encuesta....91
Figura 12. Tiempo de vinculación en la empresa....91
Figura 13. Tipo de contrato....92
Figura 14. Uso de la información....93
Figura 15. Teletrabajo en la organización....94
Figura 16. Credenciales de acceso a los sistemas....94
Figura 17. Uso de cifrado....95
Figura 18. Uso de backup de archvos....95
Figura 19. Acceso físico controlado....96
Figura 20. Uso de software antivirus....97
Figura 21. Cifrado de equipos....97
Figura 22. Características de los equipos....98
Figura 23. Capacitación interna sobre herramientas informáticas....99
Figura 24. Capacitación interna SGSI....99
Figura 25. Incidentes de seguridad....100
Figura 26. Frecuencia de incidentes....100
Figura 27. Gravedad de los incidentes....101
Figura 28. Conocimiento políticas de seguridad de la información....101
Figura 29. Identificación del responsable de seguridad....102
Figura 30. Capacitación frente a incidentes de seguridad....103
Figura 31. Cambio de contraseñas....103
Figura 32. Cambio obligatorio de contraseña....104
Figura 33. Actualización de equipos....104
Figura 34. Bloqueo de equipos....105
Figura 35. Percepción sobre las medidas de seguridad....105
Figura 36. Uso de medios extraíbles....106
Figura 37. Cuidado de las contraseñas....107
Figura 49. Carta aceptación de la empresa....293

LISTA DE TABLAS

Cuadro 1. Cuadro de delitos y leyes colombianas 72
Cuadro 2. Metodología de Investigación 81
Cuadro 3. Planear 82
Cuadro 4**.** Diseño del SGSI 83
Cuadro 5. Implementación 84
Cuadro 6. Población 86
Cuadro 7. Valoración de activos 111
Cuadro 8. Inventario de Activos y Valoración 111
Cuadro 9. Valoración de la probabilidad de ocurrencia 113
Cuadro 10. Selección y valoración de amenazas 114
Cuadro 11. Clasificación del Riesgo 130
Cuadro 12. Cálculo del riesgo 130
Cuadro 13.Nivel de madurez de salvaguardas 165
Cuadro 14. Salvaguardas seleccionadas 165
Cuadro 15. Diagnóstico inicial de documentación. 258
Cuadro 16. Diagnóstico inicial políticas de seguridad de la información 260
Cuadro 17. Diagnóstico inicial de recursos humanos 260
Cuadro 18. Diagnóstico inicial de gestión de activos 261
Cuadro 19. Diagnóstico inicial de control de acceso 261
Cuadro 20. Diagnóstico inicial de criptografía 262
Cuadro 21. Diagnóstico inicial de seguridad física 262
Cuadro 22. Diagnóstico inicial de equipos 263
Cuadro 23. Diagnóstico inicial de operaciones 263
Cuadro 24. Diagnóstico inicial de comunicaciones 265
Cuadro 25. Diagnóstico inicial adquisición, desarrollo y mantenimiento de sistemas. .265
Cuadro 26. Diagnóstico inicial de incidentes de seguridad 266
Cuadro 27. Diagnóstico inicial de Proveedores 266
Cuadro 28. Diagnóstico inicial de continuidad 267
Cuadro 29. Diagnóstico inicial de cumplimiento 267
Cuadro 30. Inventario de activos 269
Cuadro 31. Respuestas Encuesta Parte 1 276
Cuadro 32.Respuesta Parte 2 280
Cuadro 33. Respuestas Parte3 284
Cuadro 34. Respuestas Parte 4. 288

LISTA DE ANEXOS

ANEXO A. DIAGNÓSTICO INICIAL DOCUMENTACIÓN 258
ANEXO B. DIAGNÓSTICO INICIAL PROCESOS Y DOMINIOS 260
ANEXO C. INVENTARIO DE ACTIVOS 269
ANEXO D. ACEPTACIÓN EMPRESA 271

GLOSARIO

ACTIVO**:** Se conoce como activos de la información a todos los recursos necesarios para que una organización funcione y alcance objetivos o metas, genere un servicio, tome decisiones, entre otros.

ACIS**:** Asociación Colombiana de Ingenieros de Sistemas.

CIBERSEGURIDAD**:** Se considera como una "capa de protección para los archivos de información", enfocándose en la implementación de sistemas robustos, seguros y estables.

CIBERCRIMEN**:** Actividades ilícitas por las cuales un atacante o cibercriminal puede acceder a información de forma no autorizada, como códigos de acceso, números de cuentas, información personal, o para realizar actividades no permitidas como envío de spam, ingeniería social, ataques a redes y ordenadores.

COBIT**:** Siglas en español para Objetivos de Control para la Información consiste en un conjunto de prácticas que ayuda a las organizaciones en el cumplimiento de objetivos y eficiencia a nivel de Tecnología de la Información.

CONTACT CENTER: Centro de Contacto, usualmente hace referencia al área (y en muchos casos otras empresas de servicios) encargadas de la gestión de comunicaciones con los clientes.

CONTROL**:** Un control es un término que engloba diferentes tipos de acciones, documentos, medidas, procedimientos, que permiten garantizar la gestión correcta de una vulnerabilidad o amenaza descubierta en un sistema.

CORE BUSINESS**:** Actividad o negocio principal de una empresa u organización.

CRM**:** Siglas de Customer Relationship Management o Gestión de Relaciones con Clientes, es un concepto aplicado al software que permite dicha gestión en las empresas.

ESTÁNDAR**:** el término estándar se aplica para un modelo, una práctica, un patrón que se puede aplicar de forma general para medir, valorar o ejecutar algo.

IEC**:** *International Electrotechnical Commision* – Comisión electrotécnica internacional.

IOT: *Internet of Things* - Internet de las cosas.

ISO**:** *International Organization of Standarization* – Organización internacional de la normalización.

ITIL**:** *IT Infraestructure Library* – Biblioteca de Infraestructura de TI.

MINTIC: Ministerio de las Tecnologías de la Información y Comunicación.

POLÍTICA**:** Describe una posición, una guía, en general de obligatorio cumplimiento.

PROCEDIMIENTO**:** Método o forma de realizar determinadas acciones.

SGSI**:** Sistema de Gestión de Seguridad de la Información.

RESUMEN

Las empresas de Contact Center son organizaciones enfocadas en la "tercerización" de servicios, modalidad en la cual las organizaciones cliente se pueden dedicar a su Core Business entregando a otra empresa la responsabilidad sobre procesos complementarios o de apoyo, de esta forma se aprovecha la experiencia y preparación de proveedores en determinadas tareas (CRM, IT, Logística, entre otros) y se ahorra en recursos, esfuerzo y tiempo. Las empresas que actúan como proveedor de servicios de CRM reciben de sus clientes un activo que en los últimos años ha tomado una relevancia cada vez más importante, la información, con el compromiso de garantizar su buen uso, cuidado, transmisión, almacenamiento.

El propósito de este proyecto de grado aplicado es diseñar para el área de Tecnología de la Información (TI) de Telemarketing S.A.S (nombre ficticio usado para hacer referencia a la empresa sobre la que se realiza este proyecto para preservar su privacidad) un Sistema de Gestión de Seguridad de la Información que le permita cumplir con las condiciones que aseguren en el manejo de la información la confidencialidad, integridad y disponibilidad, lo cual le permitirá mejorar sus procesos operativos (el acceso y uso eficiente de la información para sus labores de Contact Center, toma de decisiones, definir estrategias de negocio, entre otras) al tiempo que ofrece a sus clientes la tranquilidad y confianza (que al final repercute en la imagen del proveedor).

Para llevar a cabo esta tarea se toma como base la norma ISO\IEC 27001:2013 y se ejecutan las diferentes actividades que permiten el diseño del SGSI; partiendo por el levantamiento de inventario se han clasificado los activos en diferentes grupos (esenciales, personal, instalaciones, servicios subcontratados, servicios internos, aplicaciones y equipos) y se han valorado de acuerdo con su relevancia en la operación de la organización (siendo precisamente los activos directamente relacionados con la operación los de más alto valor mientras los relacionados con áreas de apoyo los de menor importancia).

El análisis de riesgos y amenazas (basado en la probabilidad de ocurrencia, nivel de degradación e impacto posible) ha permitido llegar a la identificación de los problemas de la empresa en cuanto a seguridad de la información, siendo los más destacables la falta de capacitación del personal, la falta de control de uso de los recursos informáticos, y de forma muy crítica la gestión de las copias de seguridad.

Con base en los hallazgos realizados en la etapa de análisis de riesgos y amenazas se ha realizado la selección de salvaguardas, controles y políticas (incluida la política general de sistema de gestión de seguridad de la información), el alcance del sistema,

los objetivos del SGSI, todo conformando el sistema de gestión de seguridad de la información propiamente dicho.

Palabras Clave: SGSI, SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, GESTIÓN DE ACTIVOS, ANÁLISIS DE RIESGOS, CONTROLES DE SEGURIDAD, POLÍTICAS DE SEGURIDAD, 27001:2013

ABSTRACT

Contact Center enterprises are organizations focused on the “outsourcing” services, modality in wich client organizations can dedicate themselves to their main business, giving to another company the responsibility about complementary or support process, on this way they can take advange of providers experience and preparation on specific taks (CRM, IT, Logistics, and others) and save resouces, effort and time. Enterprises that act as providers of CRM services receive from their clients an asset that in recent years has taken on a increasingly important relevance, the information, with the commintment to guarantee it’s good use, care, transmision, storage.

This application degree proyect’s purpose is to design for The Information Techonology Area (IT) of Telemarketing S.A.S (ficticious name used to refer to the organization on wich this project is carried out to preserve their privacy) an Information Security Management System that allows them to comply with conditions that ensure confidentiality, integrity and availability in the information handling, wich will allow them to improve their operational process while offering their clients peace of mind and trust (wich ultimately affects the supplier image).

To carry out this task, the ISO/IEC 27001:2013 standard is taken as the basis and different activities that allow the desing of the ISMS are executed; started from the inventory survey, the assets have been classified into different groups (essential assets, staff, facilities, subcontracted services, internal services, applications and equipment) and have been valued according to their relevance in the organization's operation (the assets directly related to the operation are those of the highest value while those related to support areas those of less importance).

The analysis of risks and threats (based on the probability of occurrence, level of degradation and possible impact) has allowed the identification of the company's problems in terms of information security, the most notable being the lack of training of the staff, the lack of control of the use of computing resources, and very critically the management of backups.Based on the findings made in the risk and threat analysis stage, the selection of safeguards, controls and policies (including the general policy of the information security management system), the scope of the system, the objectives of the ISMS, all forming the information security management system itself.

KeyWords: ISMS, INFORMATION TECHNOLOGY MANAGEMENT SYSTEM, ASSET MANAGEMENT, RISK ANALYSIS, SECURITY CONTROLS, SECURITY POLITICS, 27001:2013

INTRODUCCIÓN

Ha pasado tiempo desde que los sistemas de información hicieron su entrada triunfal en los procesos cotidianos tanto a nivel de las empresas como de los hogares y es que después de la revolución industrial inició la revolución tecnológica y su influencia ha marcado las generaciones pasadas y presentes; probablemente muy pocas personas pueden imaginarse realizar sus actividades diarias sin elementos que de cualquier forma involucran algún "componente" informático, tal como se menciona en los siguientes ejemplos:

- El comercio ha pasado del almacén físico al virtual, las tiendas on-line entran cada vez más fuerte (aun cuando muchas personas se sienten muy prevenidas con la compra en estos sitios) y la posibilidad de hacer compras fuera del ámbito local brinda muchas posibilidades tanto para compradores como para vendedores que pueden de un lado acceder a más y mejores alternativas en productos y servicios, mientras que por el otro los negocios pueden expandirse y llegar a lugares que en tiempos anteriores ni se hubieran imaginado. En la actualidad acciones tan simples como ver la cartelera de cine y comprar una entrada para ver una película se pueden hacer desde el mismo sitio web.

- La educación también ha cambiado de una forma significativa, por un lado mucho material educativo puede ser encontrado en Internet permitiendo al estudiante tener documentación a la mano y de forma más inmediata (libros, videos, audios, noticias, etcétera), pero también la acogida de la formación virtual ha sido importante y ha permitido llevar a todos los rincones del mundo (que cuenten con una conexión de Internet) oferta educativa desde la básica primaria hasta la especialización profesional.

- Por otro lado, las empresas actuales han visto como el papel del activo importante ha pasado a ser de la información, teniendo en cuenta además que los sistemas informáticos son la base sobre la cual trabaja y se mantiene. A partir de la información las empresas actuales toman decisiones significativas para su presente y futuro, pueden hacer proyecciones o realizar acciones específicas en pro de mejorar su situación o tener una ventaja en el mercado. Otras organizaciones incluso basan su negocio netamente en la información, en el tratamiento de datos, o en su protección.

Aun cuando los sistemas de información son parte fundamental de las actividades cotidianas vale la pena señalar que en cuanto a la protección de los mismos parece que aún falta mucho camino por recorrer, especialmente para Colombia, donde muchas

empresas no le dan la importancia suficiente a la protección de la información, algo que se presenta especialmente por ser un elemento que requiere de una inversión que no retorna de una forma tangible para la organización y solo se dan cuenta de la enorme relevancia que tiene este aspecto cuando ya existe una pérdida de datos, ya sea de forma accidental o por un ataque directo, y ahí es cuando se ve el efecto sobre su economía: puede ser debido a multas o sanciones impuestas por organismos de control o por clientes que pierden la confianza en la empresa, o incluso por la toma de malas decisiones debido a falta de información confiable y suficiente para hacerlo.

En materia de seguridad de la información existe ya un camino trazado considerando los avances importantes que en esta materia se han desarrollado fruto de las experiencias acumuladas en todo tipo de organizaciones a nivel mundial que se han dado cuenta de lo que significa proteger la información, las cuales a su vez a su vez han alimentado a través de sus prácticas a otras organizaciones y han permitido construir normas y metodologías que buscan facilitar la tarea de implantar un Sistema de Gestión de Seguridad de la Información de una forma no solo efectiva, sino lo más simple posible y completamente documentado, verificable y con capacidad de mejorar y evolucionar en el tiempo. Así entonces las organizaciones actuales pueden hacer uso de:

- ISO\IEC 27000
- Ley de Protección de Datos
- Ley de Propiedad Intelectual
- ITIL
- COBIT
- Estándar 17999
- Leyes de Delitos Informáticos (Ley 1273 de 2009)
- BS 25999 (Plan de continuidad del negocio)
- Modelo Bell-LaPadula, entre otros

El diseño de un SGSI implica inversión y esfuerzo(al igual que su futura implementación), algo que no todas las empresas pueden o quieren asumir ya que implica destinar un presupuesto e incluso un grupo de personas dedicada a la seguridad de la información, acciones que usualmente solo son consideradas por grandes empresas u organizaciones que ya han sido atacadas, como lo menciona la Revista Dinero (Edición Electrónica) haciendo un análisis de la 'Encuesta Anual de Seguridad de la información' titulado adecuadamente como ***Las empresas colombianas escatiman gastos en gastos y se rajan en ciberseguridad***" y en el que la vocera de EY Colombia, María Conchita Jaimes señala respecto al tema de la ciberseguridad que "Las empresas colombianas lo han ido entendiendo y se han hecho avances, sin embargo la evolución de las técnicas del cibercrimen es acelerada y se deben hacer mayores esfuerzos económicos y técnicos

para enfrentarlas y reducir su impacto"[1] y que contrasta con la afirmación de la revista en cuanto a que "A pesar de que los expertos aseguran que los criminales y trampas cibernéticas aumentarán y tendrán nuevas formas de lograr sus delitos, el 59% de las empresas en el país indicó que para los siguientes 12 meses podrían hacer recortes en el presupuesto que tiene para ese rubro o lo mantendrán congelado"[2] , es decir que las técnicas de ciberataques evolucionan, mejoran y crecen pero no lo hace en la misma medida los esfuerzos para contrarrestarlas pues las organizaciones permanecen en el mismo punto o incluso disminuyen sus esfuerzos . Un estudio del presente año realizado por el Tanque de Análisis y Creatividad de las TIC (TicTac)[3]-[4], una organización establecida por la Cámara Colombiana de Informática y Telecomunicaciones (CCIT) -y citada a su vez por la revista Dinero en el artículo relacionado anteriormente- muestra que más del 80% de las organizaciones que gestionan mediante el tratamiento de datos no cuentan con un sistema de gestión de la seguridad de la información, algo especialmente en una época en que los incidentes de seguridad han crecido notablemente (se reporta un incremento del 8% en el primer trimestre de 2020 y hasta un 37% en la primera semana de abril del mismo año).

Bajo ese panorama es importante recordar que ninguna empresa está exenta de sufrir las consecuencias de un ataque informático o incluso de un accidente en sus sistemas informáticos, y es un hecho que las organizaciones que no cuentan con un sistema de seguridad se encuentran más expuestas debido a que no tienen dentro de sus programas y planes de crecimiento la preparación, procedimientos y otros elementos que les permitan hacer frente ante una falla o ataque, lo cual puede suceder bien sea por ignorancia, descuido o porque su situación económica actual (no han logrado el punto

---

[1] ALMANZA JUNCO, A. (2017). Encuesta nacional de seguridad informática 2017. Obtenido de Revista Sistemas: http://acis.org.co/revista143/content/encuesta-nacional-de-seguridad-inform%C3%A1tica-2017

[2] IBID

[3] TANQUE DE ANÁLISIS Y CREATIVIDAD DE LAS TIC (TICTAC) - CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES CCIT. (29 de 10 de 2019). *Tendencias Cibercrimen Colombia 2019-2020*. Obtenido de CCIT.org.co: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-final.pdf

[4] TANQUE DE ANÁLISIS Y CREATIVIDAD DE LAS TIC (TICTAC) - CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES CCIT. (04 de 2020). *Informe Tendencias del CiberCrimen Primer Trimestre 2020.* Obtenido de CCIT.org.co: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-abril-2020-final.pdf

de equilibrio, por ejemplo) no se los permite. Pero hoy en día existen incluso casos en los cuales una empresa supera el punto de equilibrio y entra en un momento de bonanza y crecimiento, pero se han acostumbrado a "vivir" sin depender de un SGSI (incluso de un sistema de gestión de calidad como ISO 9000) por lo que finalmente asumen que no lo necesitan, hasta que llegan los problemas.

Es un hecho que en Colombia (y probablemente en casi todo el mundo) el camino de las empresas no es simple, y si sus sistemas de información no son seguros lo será mucho menos, puesto que existen muchas personas afuera que solo están esperando cualquier espacio para tratar de obtener información o simplemente superar "retos" personales que al final pueden terminar en desastre para aquellos que no están preparados para enfrentar estas situaciones (eso sin contar los retos a nivel logístico, económico, entre otros, que se pueden encontrar en su día a día). De acuerdo con una publicación de la revista Gerente en abril de 2016 y al publicado en el blog Ciberseguridad (ciberseguridad.blog) las empresas se enfrentan a retos como los siguientes[5] [6]:

- Los ataques están principalmente enfocados en el intento de fraudes electrónicos, el robo de información sensible, el espionaje industrial o el bloqueo de servicios.

- Los ataques están afectando con más fuerza el buen nombre y la reputación de las organizaciones; se puede citar el caso de Facebook como ejemplo de lo que genera una noticia de la perdida (o mal uso de la información) en una empresa con influencia a nivel mundial.

- Los ataques se vuelven cada vez más sofisticados, hay no solo mayor conocimiento en las personas que los realizan sino un mayor nivel de estudio y planificación por parte de los atacantes.

- Se identifican 5 tendencias relacionadas con la seguridad de la información:

    - Internet de las cosas (IoT): muchos dispositivos conectados y pocas capacidades de seguridad.

[5] CIFUENTES, A. (22 de 12 de 2017). *Retos de ciberseguridad para las compañías en el 2018*. Obtenido de Gerente.com: http://gerente.com/co/rciberseguridad-companias-2018/

[6] MELON, L. (12 de 12 de 2017). *Los 5 retos clave para la ciberseguridad en 2018*. Obtenido de Ciberseguridad.blog: https://ciberseguridad.blog/los-5-retos-clave-para-la-ciberseguridad-en-2018/

- Cadena de suministro: La información se "mueve" entre diferentes puntos, se comparte entre diferentes organizaciones, se almacena en diferentes formatos, y en todo este proceso se generan riesgos para la misma.

- Crimen informático como servicio (CaaS): Existen actualmente organizaciones dispuestas a ofrecer sus "servicios" enfocadas en distintos tipos de ataques.

- Nuevas regulaciones: En el mismo proceso de mejorar las condiciones de seguridad de la información y de las entidades se crean regulaciones o se modifican las existentes lo cual genera un reto para las organizaciones que tienen que adaptarse.

- Expectativas al interior de las organizaciones: existe un problema de educación o conocimiento en las organizaciones en lo que a seguridad de la información respecta, lo cual supone una barrera o por lo menos complicaciones a la hora de intentar implementar o mantener un SGSI o cualquier otra metodología o estándar.

Considerando lo visto hasta acá se identifica lo importante que resulta para las empresas que realicen un análisis de su situación actual en cuanto a seguridad de la información se refiere: ¿qué avances se han dado específicamente para esta área de TI? y ¿qué puntos siguen siendo débiles al respecto? Posteriormente se pueden buscar o identificar alternativas que les permitan superar estas debilidades (al hablar de seguridad de la información los términos más adecuados son controlar y protegerse) de tal forma que puedan ser más competitivas y seguras en el ámbito actual. Es precisamente el objetivo de este trabajo permitir a la empresa Telemarketing S.A.S realizar un proceso en el área de TI que le permita identificar los elementos que le permitan mejorar su seguridad al contar con el diseño de un SGSI.

1 DEFINICIÓN DEL PROBLEMA

1.1 PRESENTACIÓN DEL TEMA

La información se ha convertido en un activo importante para las organizaciones actuales, ya sea incluida dentro del objeto de negocio, para la toma de decisiones o como parte de la imagen corporativa y confianza que brinda hacía el cliente. No obstante, una cantidad importante de empresas no son conscientes del papel de la información en sus actividades o no dedican los recursos suficientes para protegerla de las diferentes amenazas que se pueden presentar.

Siguiendo la línea de la Especialización en Seguridad Informática se enfoca el presente trabajo en el Sistema de Gestión de Seguridad de la Información aplicado a una empresa en la cual se realizará el análisis de la organización, el diseño del SGSI y la selección de las políticas de seguridad adecuadas.

1.2 ANTECEDENTES

Los SGSI vienen funcionando ya desde un tiempo considerable y también se puede decir que el estudio de la aplicación de la seguridad de la información en las organizaciones es algo que ya ha tenido aplicación como se puede evidenciar en las encuestas realizadas por organizaciones como ACIS (Encuesta Nacional de Seguridad Informática) y de la cual se publican resultados y análisis realizados por la misma organización u otras entidades que toman los datos para extraer conclusiones y estadísticas. La situación actual de acuerdo con los resultados publicaos por ACIS en su revista muestran lo siguiente[7]:

- Herramientas de seguridad: Las evaluaciones de seguridad realizadas por el 60% de los encuestados con distintas frecuencias:

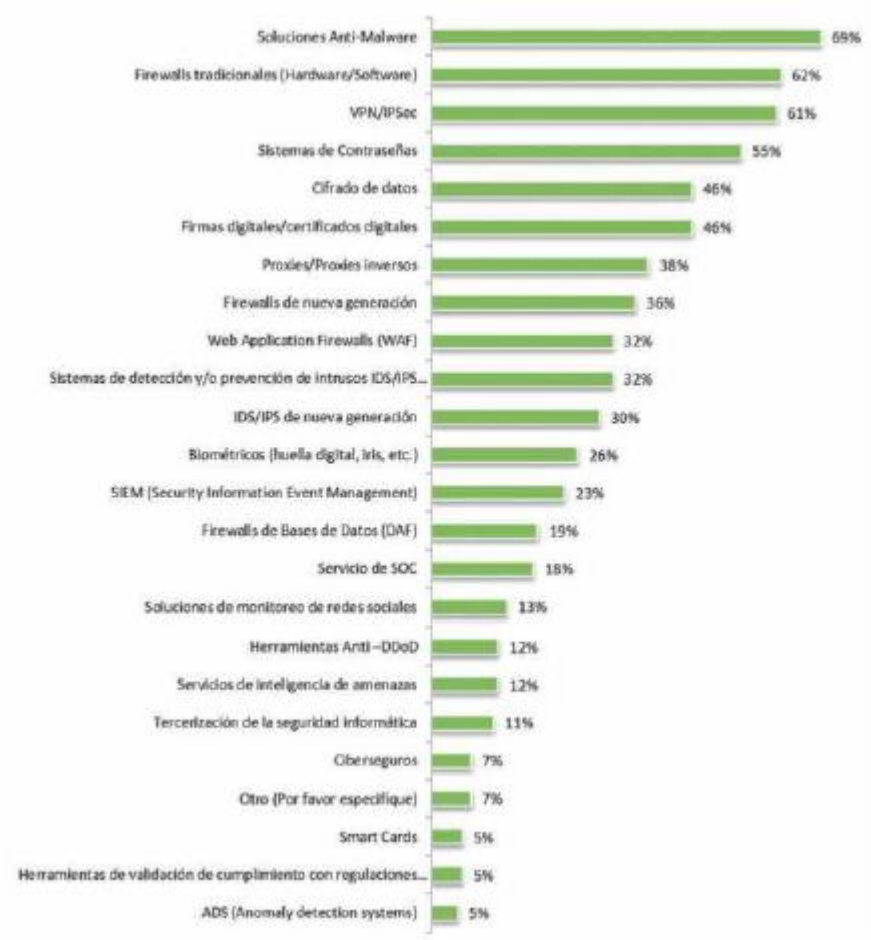
[7] ALMANZA JUNCO, A. R. (2017). *Encuesta nacional de seguridad informática 2017*. Obtenido de Revista Sistemas: http://acis.org.co/revista143/content/encuesta-nacional-de-seguridad-inform%C3%A1tica-2017

Figura 1. Evaluaciones de Seguridad

Fuente**:** (ALMANZA JUNCO, 2017)

- Soluciones de seguridad: En relación con las soluciones de seguridad usadas por las organizaciones las soluciones antimalware y los Firewall son lo más común.

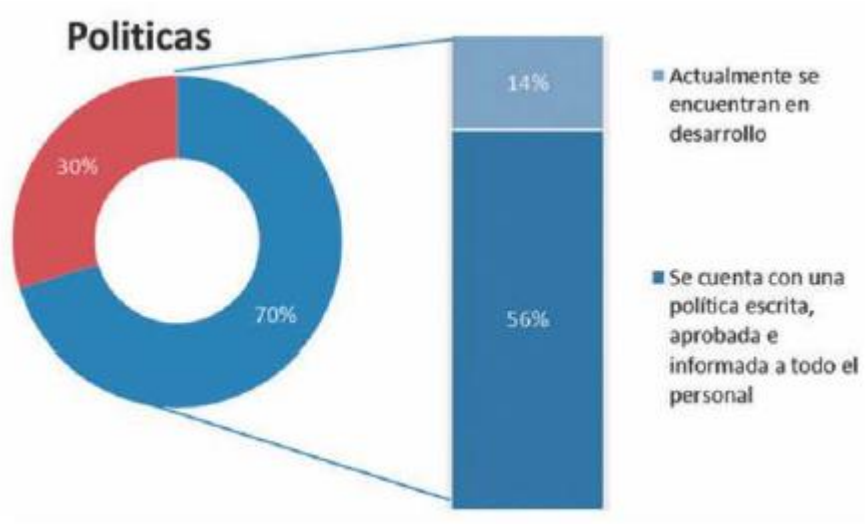
Figura 2. Soluciones de seguridad



Fuente: (ALMANZA JUNCO, 2017)

- Políticas de seguridad: Se puede decir que el panorama respecto al uso de políticas de seguridad la situación actual es buena, considerando que el 70% de las organizaciones encuestadas las están desarrollando (14%) o las tienen completamente desarrolladas (56%). No obstante, hay que mencionar que esto contrasta con las afirmaciones de otras entidades que mencionan que las empresas en Colombia aún tienen problemas serios en materia de ciberseguridad, quedando en el aire si la aplicación de esas medidas es realmente efectiva o el nivel de compromiso de las organizaciones.

Figura 3. Políticas de seguridad



Fuente: (ALMANZA JUNCO, 2017)

- *Frameworks* de Seguridad: ISO\IEC 27001 es la normal líder en las organizaciones colombianas a la hora de buscar un *framework* sobre el cual trabajar la seguridad de la información.

Figura 4. *Frameworks* de seguridad

Fuente: (ALMANZA JUNCO, 2017)

- Obstáculos a la seguridad: Para cerrar esta parte (el informe contiene información más detalla e incluye otros ítems) es importante señalar que en la encuesta se identifica la falta de cultura en seguridad de la información como el principal obstáculo a la seguridad con el 61%. El apoyo directivo por su parte se encuentra

como el tercer obstáculo (35%) pero es superado por la falta de colaboración entre áreas y/o departamentos (40%):

Figura 5. Obstáculos a la seguridad

Fuente: (ALMANZA JUNCO, 2017)

Igualmente, revistas especializadas han realizado estudios en conjunto con organizaciones y entidades gubernamentales (MINTIC como ejemplo) en la cual se evidencia la situación de las empresas en relación con la seguridad de la información, las cuales se muestran vulnerables y mal preparadas para afrontar los retos que en este ámbito pueden encontrarse en sus actividades cotidianas.

En general se puede decir entonces que organizaciones privadas y públicas, o incluso la unión de ambos tipos de entidades, han generado previamente documentos y estudios relacionados con la seguridad de la información tanto en las empresas como en el ámbito particular, la mayoría con análisis muy generales de la situación. De la misma forma algunas empresas tanto a nivel regional como nacional ya han implementado Sistemas de Gestión de Seguridad de la Información, aplicando las políticas a diferentes niveles. A nivel académico se han realizado diferentes trabajos sobre la implementación de SGSI en organizaciones de diferentes naturalezas; entre los casos revisados en el desarrollo de este proyecto se pueden mencionar los siguientes:

- Diseño de un sistema de gestión de la seguridad de la informática –SGSI-, para empresas del área textil en las ciudades de Itagüí, Medellín y Bogotá D.C. a través

de la auditoría[8]. Este trabajo realizado por los estudiantes Alexander Guzmán García y Carlos Alberto Taborda Bedoya en el año 2015 para la especialización en Seguridad Informática de la Universidad Nacional Abierta y a Distancia – UNAD se enfoca en desarrollar un SGSI basado en la norma ISO\IEC 27001 para empresas de la industria textil tipo PyME (Pequeñas y Medianas Empresas).

El punto por destacar de este trabajo se encuentra en que considera un sector económico con dificultades en la implementación de políticas de seguridad de la información dada su situación económica que limita los recursos disponibles para llevar adelante esta tarea.

- Diseño de un sistema de gestión de seguridad de la información en el área de recursos informáticos de la contraloría departamental del Meta, según la norma ISO 27001[9]: El trabajo del Ing. Cazaran Buitrago está enfocado en el área de Recursos informáticos fundamentado en la realización del análisis de las amenazas, vulnerabilidades y riesgos de dicha dependencia para la generación de las políticas de seguridad adecuadas.

  El trabajo se basa en la aplicación de la norma ISO\IEC 27001:2013 y la metodología MAGERIT, desde los cuales se desarrollan las políticas, procedimientos, controles, plan de continuidad, entre otros elementos fundamentales para el SGSI.

A nivel de la organización en la cual se aplica el proyecto, aunque se han intentado aplicar procedimientos estandarizados aún no se cuenta con un SGSI propiamente dicho, sin embargo, la naturaleza de su negocio en el cual se involucra el uso de datos personales (entre otros tipos de información) hacen necesario contar con un Sistema de Gestión de Seguridad de la Información. Dentro de los problemas y aciertos que se conocen en la organización con relación a la seguridad de la información se pueden considerar los siguientes:

---

[8] GUZMAN GARCÍA, A., & TABORDA BEDOYA, C. A. (2015). *Diseño de un sistema de gestión de la seguridad informática -SGSI-, para empresas del área textil en las ciudades de Itagüí, Medellín y Bogotá D.C. a través de la auditoría.* Obtenido de Stadium.unat.edu.co: http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3448/1/1030548291.pdf

[9] CAZARAN BUITRAGO, O. Y. (2017). *Diseño de un sistema de gestión de seguridad de la información en el área de recursos informáticos de la contraloría departamental del meta, según la norma ISO 27001.* Obtenido de Repository.unad.edu.co: https://repository.unad.edu.co/bitstream/10596/17423/1/1121839952.pdf

- Aciertos
    - Se han aplicado buenas prácticas en algunos aspectos como:
        - Definición de roles y responsabilidades en TI.
        - Segregación de funciones y áreas de responsabilidades.
        - Inventario parcial de activos (Hardware y Software).
        - Clasificación de la información.
        - Implementación de Directorio Activo.
        - Restricciones de acceso a la información.
    - Se han delimitado zonas críticas:
        - Delimitación del perímetro de seguridad.
        - Delimitación del centro de procesamiento de datos.
        - Controles de acceso físico para las zonas críticas.
        - Controles de acceso físico para las oficinas.
        - Controles y políticas para la protección ante desastres naturales, ataques maliciosos y accidentes.
- Problemas
    - No cuenta con procedimientos documentados.
    - No cuenta con registros.
    - No existe documentación de los requisitos estatutarios, reglamentarios y contractuales.
    - La dirección no realiza revisión del cumplimiento de SGSI.
    - Falta implementación de controles.

1.3 DESCRIPCIÓN DEL PROBLEMA

Las empresas de *Contact Center* (o Centro De Atención Telefónica) tiene un compromiso importante con sus clientes debido a que sus operaciones se basan normalmente en la gestión de información personal para realizar campañas comerciales a través de llamadas telefónicas, email, chat u otros medios que se van implementando conforme la tecnología avanza. En este sentido los clientes dan un voto de confianza al Contact Center para que haga un buen uso de sus bases de datos, y a su vez la empresa necesita tener confianza en que sus procesos y los miembros de la organización cumplan y respeten la confidencialidad de la información y den un buen uso de ella.

Cuando los procesos no se cumplen, o los miembros de la organización no están alineados con la organización en cuanto a la protección de la información se pueden presentar problemas como:

- Fuga de información, datos personales, datos de clientes, de proveedores o incluso de la misma organización que llegan a manos de personas no autorizadas.
- Pérdida o borrado de los datos (bases de datos, informes, entre otros) que van en contra de la disponibilidad y la integridad de la información.
- Mal uso de la información, ocasionado por falencias en la protección y clasificación de esta.
- Mala gestión de la plataforma tecnológica que soporta el sistema informático.

Cuando estas situaciones se hacen presentes en una organización de esta naturaleza entonces se ve expuesta a diferentes problemas, algunos incluso muy críticos que podrían llevar a su cierre (y se extiende a sus empleados que pueden perder su fuente de trabajo). Entre las situaciones a las que se enfrenta un *Contact Center* se pueden citar las siguientes:

- Deterioro de la imagen pública de la empresa, lo cual a su vez le genera desventaja frente a la competencia, desconfianza ante clientes, proveedores y entes reguladores.
- Pérdida de clientes, finalización de contratos de servicios o sanciones a nivel económico (también de indicadores, beneficios, entre otros) que se pueden traducir a su vez en pérdidas económicas.
- Sanciones por parte de entes reguladores, que pueden ir desde sanciones administrativas hasta multas o incluso el cierre de la empresa.

Lamentablemente, la organización objeto del presente proyecto no cuenta con un sistema de gestión de seguridad de la información que promueva el cuidado de los datos. Actualmente cuentan con pocos procedimientos e incluso aislados, insuficientes para proteger las bases de datos y la plataforma con que operan a diario, además que no son del conocimiento de gran parte de la organización, por lo cual lo que existe en materia de seguridad no es aplicado correctamente (o no se aplica en muchos casos). Incluso la información propia del personal de la organización puede encontrarse expuesta debido a las vulnerabilidades informáticas presentes y que en algunos casos podrían escapar del

control de la organización y su efecto alcanzar otros sistemas informáticos (incluso hogares a través de virus, robos de información confidencial, entre otros).

Ante los anteriores escenarios es claro que existen diversos problemas relacionados con la poca (o nula) protección de uno de los activos más valiosos de las organizaciones de hoy: la información. Actualmente los riesgos económicos y de reputación no pueden ser ignorados y se requiere de forma urgente aplicar medidas que permitan garantizar la protección de la información y de la plataforma sobre la cual se procesa; en este caso se identifica un SGSI como la respuesta a dicha necesidad, generando mejores prácticas, aplicación de estándares, con las consecuentes mejoras en imagen del *Contact Center,* e incluso en su productividad y rentabilidad.

1.4 FORMULACIÓN DEL PROBLEMA

¿Cómo aplicar un sistema de gestión de la seguridad de la seguridad de la información, ISO\IEC 27001, para la protección de la información de organización desde el área de TI?

1.5 DEFINICIÓN

El trabajo propuesto consiste en la modalidad de proyecto aplicado enfocado el diseño DE un SGSI para una organización o empresa seleccionada.

1.6 DELIMITACIÓN

Geográficamente se ha definido su delimitación a la empresa Telemarketing S.A.S con sede principal en la ciudad de Pereira, Colombia. El proyecto se enfoca en el área de IT de la organización y la aplicación del SGSI basado en la norma ISO 27001:2013.

En relación con el tiempo se plantea un cronograma de 8 meses durante los cuales se llevará a cabo el proceso de análisis, diseño del SGSI y su implementación.

1.7 SUBTEMAS

Para el desarrollo del proyecto aplicado al diseño de un SGSI para la organización Telemarketing S.A.S se plantean inicialmente los siguientes subtemas:

- Seguridad de la información y Seguridad informática.
- Estándares de seguridad de la información.
- Normatividad y legislación relacionada con la seguridad de la información.
- Gestión de activos.
- Análisis e identificación de riesgos y amenazas.
- Selección de políticas de seguridad de la información.
- Diseño del SGSI.

1.8 RELACIÓN CON OTRAS ÁREAS DE ESTUDIO

La naturaleza de este proyecto permite que pueda ser relacionado con otras áreas como las siguientes:

- Seguridad: Se habla de un ámbito más amplio (no exclusivo de la seguridad de la información), teniendo en cuenta el concepto de robo (de datos, de activos, de información, entre otros) así como lo relacionado con los fraudes.

- Economía: En relación con la economía se puede tener en cuenta que parte de los crímenes económicos se ven reflejados en el ciber-crimen, por ejemplo, mediante el robo de datos financieros (números de tarjeta de crédito o cuentas bancarias), movimientos fraudulentos de fondos, entre otros.

- Calidad: ISO 9000 es un Sistema de Gestión de Calidad que se enfoca en el mejoramiento continuo de los procesos de una organización y que de diferentes formas se puede apoyar y sirve de apoyo para un SGSI teniendo en cuenta precisamente los conceptos de mejora continua y orden en los procesos, documentación, entre otros.

- Auditoría de Sistemas: Se involucran proceso de auditoría y control, revisión de procesos, documentación, entre otros relacionados con el SGSI.

1.9 ALCANCE

Se define el alcance del proyecto a los siguientes tres puntos:

- El proyecto se enfoca en el diseño de un SGSI.

- El proyecto se aplica a la empresa Telemarketing S.A.S, específicamente al área de TI.

- Este proyecto podría adaptarse a empresas de similar naturaleza que presten servicios de CRM.

2 JUSTIFICACIÓN

Las empresas están expuestas a una cantidad significativa de factores que ponen en riesgo su operación y su funcionamiento a largo plazo, incluidos aquellos relacionados con la información, su procesamiento, almacenamiento, transmisión y protección. Estos factores están relacionados especialmente con los cambios que las organizaciones han venido experimentando desde hace algunos años con la transformación digital, y es que para el año 2018 ya el 88% de las empresas colombianas tenía claro lo que significa la cuarta revolución industrial y el 65% había establecido una estrategia para la transformación digital[10], lo que se puede interpretar como una señal de como el sector ha venido entrando en esta nueva "era" bien sea invirtiendo en tecnologías ya establecidas o "maduras" (66%) o en tecnologías emergentes(62%)[11]; no obstante también es cierto que el camino que están recorriendo no está a salvo de dificultades (falta de conocimiento, bajos presupuestos, entre otros) que pueden hacer que esta transición no sea realmente exitosa y expuesta a riesgos.

Es importante señalar que la transformación digital hace un uso importante de tecnologías como la computación en nube, la tecnología de la información (TI), las plataformas móviles e incluso el *Machine Learning*, la inteligencia artificial, la realidad aumentada, la realidad virtual, el uso de redes sociales o el internet de las cosas (IoT)[12],lo cual involucra una cantidad importante de datos, plataformas tecnológicas y recursos técnicos que a su vez suelen ser objetivos o víctimas de la delincuencia (o ciber delincuencia): el informe de tendencias del cibercrimen en Colombia (2019-2020)[13]

[10] FUNDACIÓN UNIPYMES. (21 de 11 de 2019). *Empresas Colombianas más involucradas con la transformación digital.* Obtenido de Unipymes: https://www.unipymes.com/empresas-colombianas-mas-involucradas-con-la-transformacion-digital/

[11] IDEM

[12] POWERDATA. (s.f.). *Transformación digital. Qué es y su importancia y relación con los datos*. Obtenido de PowerData: https://www.powerdata.es/transformacion-digital

[13] TANQUE DE ANÁLISIS Y CREATIVIDAD DE LAS TIC (TICTAC) - CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES CCIT. (29 de 10 de 2019). *Tendencias Cibercrimen Colombia 2019-2020*. Obtenido de CCIT.org.co: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-final.pdf

presentado por TIACTAC[14] muestran como en el año 2019 se produjo un incremento del 54% en los incidentes de seguridad (respecto al 2018) de los cuales el phishing, la suplantación de identidad, el *malware* y los fraudes con medios de pagos.

El incremento de los ataques se puede explicar por factores como:

- Nuevas y más avanzadas técnicas de ataque.
- Son cada vez más un objetivo de posibles atacantes debido a sus vulnerabilidades y la cantidad de información que las organizaciones poseen actualmente.
- No cuentan con la visión que les permita identificar la información como un activo valioso de la organización que afecta no solo en su situación económica sino también en su reputación y credibilidad.
- Muchas organizaciones no cuentan con los recursos económicos para la implantación de un Sistema de Gestión de seguridad de la información.

El caso de la empresa Telemarketing S.A.S tiene tres factores relacionados con la naturaleza de su negocio que la pueden hacer propensa a este tipo de amenazas:

- Uno de sus principales activos o insumos es la información, particularmente datos personales de usuarios relacionados con las empresas que contratan sus servicios de CRM.
- Un alto porcentaje de su operación se basa en el uso y gestión de la información que los clientes les facilitan para el desarrollo de sus labores comerciales.
- Cuenta con una plataforma tecnológica que es la base de la operación de la organización.

Como todas las empresas, Telemarketing S.A.S busca el éxito de sus operaciones en el mediano y largo plazo que le permitan crecer como organización, pero esto también va

[14] TANQUE DE ANÁLISIS Y CREATIVIDAD DE LAS TIC (TICTAC) - CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES CCIT. (04 de 2020). *Informe Tendencias del CiberCrimen Primer Trimestre 2020.* Obtenido de CCIT.org.co: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-abril-2020-final.pdf

de la mano con la confianza que pueda brindar a sus clientes en el manejo de la información y en el correcto uso de esta. En este sentido la información ha pasado a convertirse en un activo de gran importancia que debe ser correctamente administrado y protegido, y para lograrlo se propone las siguientes actividades para el presente trabajo:

- Realizar un análisis de la situación actual de la empresa en cuanto a seguridad de la información.
- Identificar las falencias que presentan la organización en cuanto a seguridad de la información.
- Seleccionar unas políticas generales que respondan a las falencias detectadas.
- Diseñar un SGSI para la organización en el área de TI.

Con esto se busca mejorar las condiciones de la organización, disminuyendo los niveles de inseguridad actual en relación con seguridad de la información, de tal forma que pueda continuar siendo competitiva, mejorar su nivel de confianza frente a clientes y entes de control, y disponer de información más efectiva que permita la toma de decisiones.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar un Sistema de Gestión de Seguridad de la Información en base a la norma ISO\IEC 27001:2013 para el área de TI de la empresa Telemarketing S.A.S. que les permita contar con un nivel de seguridad de la información adecuado.

3.2 OBJETIVOS ESPECÍFICOS

- Realizar el levantamiento del inventario de activos informáticos de la empresa y la valoración de los activos de la organización.
- Realizar el análisis de riesgos y amenazas de los activos informáticos de la organización mediante la aplicación de la metodología MAGERIT.
- Identificar los problemas de seguridad de la información que se presentan en el área de TI de la organización.
- Seleccionar un conjunto de políticas y controles basados en el Sistema de Gestión de Seguridad de la Información acordes a los problemas identificados.
- Definir los roles dentro de la organización que estarán relacionados con el SGSI para el área de TI de la organización y sus responsabilidades en la gestión del SGSI.
- Definir la política de SGSI, así como su alcance y objetivos.
- Diseñar el SGSI basado en la norma ISO\IEC 27001:2013 para el área de TI de la empresa Telemarketing S.A.S considerando las políticas y controles seleccionados.

4 MARCO REFERENCIAL

4.1 MARCO CONTEXTUAL

4.1.1 Descripción de la empresa. Telemarketing S.A.S es una entidad privada enfocada en la prestación de servicios de *Contact Center* con sedes en Colombia y Perú, además de poseer una amplia experiencia en los sectores de Telecomunicaciones, *fundraising*, útiles, banca y seguros. La organización cuenta con más de 500 empleados, además de una estructura organizacional que incluye departamentos propios de TI, calidad y formación.

Su mayor fortaleza se encuentra en el capital humano y la experiencia en el sector de *Contact Center*, sumado a su capacidad de ofrecer servicio 24 horas al día, 7 días a la semana, los 365 días al año, y de ser una de las organizaciones del sector con índices de rotación reducidos, lo que genera una importante estabilidad en el personal. Se destaca también su capacidad de organización, flexibilidad y rápida adaptación a las necesidades de los clientes.

4.1.2 Misión. Prestar servicios de Contact Center, por medio de procesos que integran la innovación, la experiencia y un amplio despliegue tecnológico, logrando con ello la satisfacción del cliente, superando sus expectativas, y cumpliendo con los estándares de calidad exigidos.

4.1.3 Visión. Ser reconocido como una de las empresas líderes del sector, caracterizada por la calidad, el profesionalismo y la innovación en la prestación de cada uno de sus servicios.

4.1.4 Valores. Los valores asociados a Telemarketing S.A.S son los siguientes:

- Responsabilidad.
- Honestidad.
- Liderazgo.
- Mejora continua.
- Integridad.
- Confidencialidad.

4.1.5 Áreas de negocio. Telemarketing S.A.S presenta dos áreas de negocio identificadas dentro de la gestión de Contact Center, la gestión de Inbound mediante la cual se reciben las peticiones de los clientes y la gestión de Outbound mediante la cual se hace seguimiento y venta de servicios.

- Inbound:
    - Atención al cliente.
    - Soporte comercial y de ventas.
    - Soporte y asistencia técnica.
    - Gestión de agendamientos.
    - Gestión de pedidos.
    - Registro de datos.
    - IVR Interactive Voice Recorder.
    - Retención.

- Outbound:
    - Telemercadeo.
    - Recobros.
    - Verificaciones.
    - Encuestas.
    - Captación de clientes – Clic to Call.
    - Tele-concertación de citas.
    - Migraciones.
    - Campañas de fidelización.
    - Actualización y cualificación de BBDD (bases de datos)

Adicionalmente la organización apoya sus servicios en:

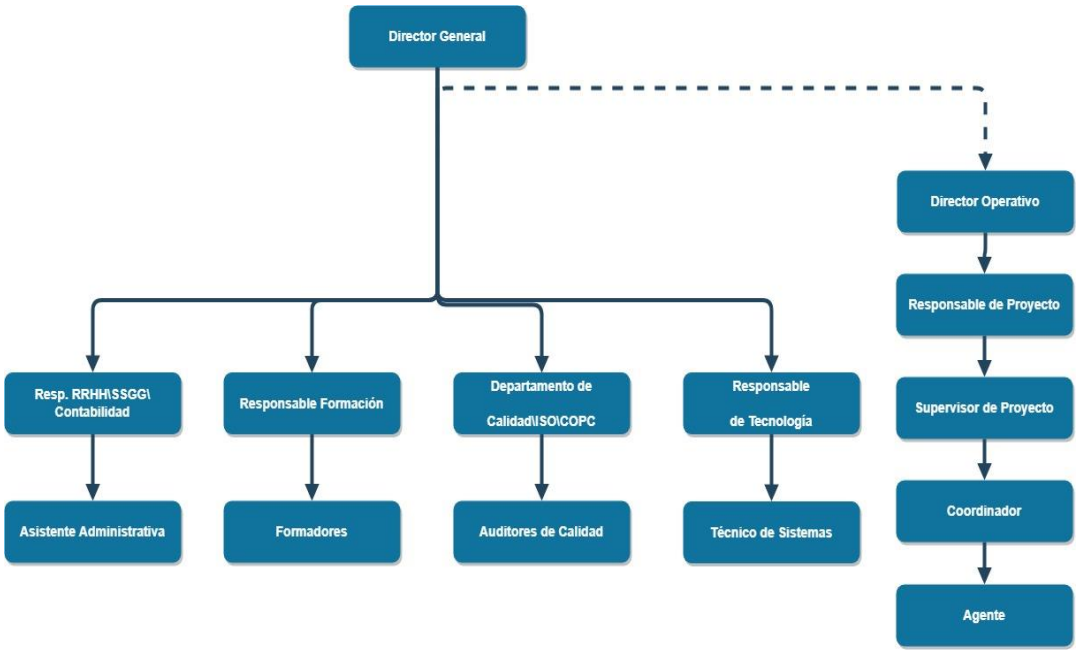
- Back-office: apoyo a nivel de tramitación y gestión documental, tramitación de incidencias, gestión y respuesta de mails.

- BBDD (Bases de datos): Gestión y optimización de BBDD de clientes, departamento de Inteligencia Empresarial, BBDD propias.

- Mercado Digital: Externalización de la realización gráfica para editoriales del mercado de habla hispana y portuguesa, tanto para productos impresos como para productos digitales.

4.1.6 Organigrama. Organigrama de la empresa

Figura 6. Organigrama Telemarketing S.A.S



Fuente: Telemarketing S.A.S

4.1.7 Ubicación física. La empresa Telemarketing S.A.S tiene sedes en [15]

- Colombia, Pereira – Risaralda.
- Colombia, Manizales – Caldas.
- Perú, Lima – Lima.

4.1.8 Área de TI dentro de la organización constituye una de las áreas de soporte al núcleo operativo, brindando el apoyo en cuanto a:

- Soporte a usuario final.
- Gestión de telecomunicaciones.

[15] Por motivos de seguridad no se incluyen las ubicaciones reales de la organización.

- Gestión y soporte de servidores.
- Gestión y soporte de redes.
- Desarrollo de scripts en las plataformas de marcación.
- Desarrollo de módulos php, javascript, entre otros, para apoyo a la operación mediante vistas de indicadores, reportes, etcétera.
- Gestión de usuarios.

Esta área está directamente subordinada a la Gerencia de la organización y gestiona las tres sedes mediante células coordinadas por un jefe o Gerente de TI, (cada célula se encuentra integrada por al menos 1 Técnico de TI, nombre que se designa al cargo pero que no tiene necesariamente relación con el nivel profesional del empleado).

Este mismo Gerente de TI, es a su vez responsable de velar por la seguridad de la información y de los recursos informáticos.

4.2 MARCO TEÓRICO

4.2.1 Incidentes de seguridad. Los incidentes de seguridad, de acuerdo con el sitio web CESPI[16], se describen como las acciones que no son parte de la operación normal de los servicios de TI, o incluso de la organización en general, y que, cuando se presentan, generan diferentes problemas, bien sea la interrupción de las operaciones, perdida de información, entre otros efectos. Aunque los incidentes de seguridad son variados y su cantidad crece conforme pasa el tiempo, a continuación, se describen los más relevantes según la Encuesta Nacional de Seguridad Informática del año 2015[17].

4.2.1.1 Software no autorizado. El problema del software no autorizado tiene muchas implicaciones, ya sea desde el ámbito legal como el de la seguridad, y es que, aunque no siempre, suele suceder que se ambas situaciones se encuentren ligadas. El Instituto Nacional de Tecnologías de la Comunicación (INTECO) publicó en mayo de 2012 el

[16] CESPI UNLP. (s.f.). *Incidentes informáticos*. Obtenido de CESPI: http://www.cespi.unlp.edu.ar/incidentes

[17] ALMANZA JUNCO, A. R. (06 de 2015). *Tendencias 2015 Encuesta nacional de seguridad informática. 15 años después.* Obtenido de Revista Sistemas: http://52.1.175.72/portal/sites/all/themes/argo/revista/Sistemas135.pdf

estudio sobre riesgos de seguridad derivados del software de uso no autorizado[18] en el cual se exponen las diferentes situaciones derivadas de una práctica que es difícil de erradicar de las organizaciones. Para iniciar se debe tener en cuenta el impacto económico que se genera debido a la obtención no autorizada (lo que normalmente se conoce como piratería), puesto que no se está pagando por el trabajo y esfuerzo de las empresas y desarrolladores que han desarrollado el producto. Tal como lo señala el documento[19]: "Se debe tener en cuenta que la utilización de software no autorizado no solo está considerada un delito y una violación a los derechos de autor, sino que además tiene un impacto significativo en la compañía". En este tema juega mucho la cultura y el conocimiento de los usuarios, pues muchas personas no son conscientes de los temas asociados a las licencias de uso de del software y suelen guiarse por lo que encuentren en internet, es decir, si está disponible en Internet consideran es gratuito (que debe diferenciarse del concepto de software libre). El estudio indica que[20] "El consumidor, ante la necesidad de un programa informático, en un 66,4% de los casos recurre a Internet, aunque apenas un 26,3% lo hace en un sitio oficial del producto" y adicionalmente indican "Por regla general los usuarios españoles no tienen claro cuando la adquisición del software es legal o no"[21], algo que se puede generalizar con usuarios de otros países, como Colombia.

Otro aspecto a considerar es el de los incidentes de seguridad asociados a la instalación de software no autorizado, y es que descargar un software "pirata" desde el internet conlleva una serie de riesgos, puesto que para poder hacer funcionar una aplicación que normalmente está sujeta a una licencia se hace uso de prácticas como el "crackeo" que no solo permiten que el software descargado funcione sino que también puede realizar otras actividades en el ordenador (entre ellas instalar aplicaciones "extras" que el usuario ni se entera que están corriendo en su ordenador). En otros casos el software puede venir incluso modificado, y es que de acuerdo con el estudio realizado por INTECO[22] "El software obtenido a través de estas fuentes, en su mayor parte, corresponde a programas informáticos que no están sometidos a un control estricto de distribución ni a ningún otro mecanismo que garantice la autenticidad e integridad de la descarga realizada en relación con el producto original. En ocasiones, bajo la apariencia de contenidos

[18] PÉREZ SAN-JOSÉ, P., GARCÍA PÉREZ, I., ÁLVAREZ ALONSO, E., DE LA FUENTE RODRÍGUEZ, S., & GUTIÉRREZ BORGE, C. (11 de 06 de 2012). *Estudio sobre riesgos de seguridad derivados del software no autorizado.* Obtenido de Biblioteca Escolar Digital: http://bibliotecaescolardigital.es/comunidad/BibliotecaEscolarDigital/recurso/estudio-sobre-riesgos-de-seguridad-derivados-del/61000a84-88e3-449e-83e8-e1a0e34d16ca

[19] IDEM
[20] IDEM
[21] IDEM
[22] IDEM

atractivos para los usuarios se camufla código malicioso facilitando la diseminación de este", por ejemplo:

- Troyanos o caballos de Troya.
- Adware o software publicitario.
- Herramientas de intrusión.
- Gusano.
- Spyware.
- Virus.
- Exploits.
- Rootkits.
- Scripts.
- Jokes o Bromas.

4.2.1.2 Virus\Caballo de Troya. De acuerdo con la página PANDA SECURITY[23], los caballos de Troya son un tipo de programa maligno que disfrazados de un archivo legítimo ingresan en el ordenador provocando daños al eliminar archivos, enviar información privada a ubicaciones externas no autorizadas, capturar datos ingresados por el usuario a través del teclado, etcétera. Ejemplos de troyanos son[24]:

- Netbus.
- Back Orifice 2000.
- SubSeven.
- Cybersensor.
- Deep Throat v2.
- Dolly Trojan.
- Girlfriend.
- nCommand v1.0.
- NetSpher.

[23] PANDA MEDIACENTER. (10 de 12 de 2013). *¿Qué es un troyano?* Obtenido de Panda MediaCenter: https://www.pandasecurity.com/spain/mediacenter/consejos/que-es-un-troyano/

[24] SEGURIDAD PC. (s.f.). *Concepto de troyanos informáticos*. Obtenido de SeguridadPC: http://www.seguridadpc.net/troyanos.htm

4.2.1.3 Virus informático. Según PandaSecurity[25] un virus informático actúa de forma similar a los virus biológicos, es decir se propaga mediante la infección de archivos, replicándose para llegar a más huéspedes. Dentro de equipo se seguirá reproduciendo al tiempo que puede provocar daños y pérdida de información. Una de las características para tener en cuenta con los virus es que "un virus no puede continuar su propagación sin la acción humana, (por ejemplo, ejecutando un programa infectado)"[26] .

La diferencia entre el virus y el troyano es que este último no tiene la capacidad de reproducirse, no pueden infectar archivos, es por eso por lo que requieren disfrazarse de archivos legítimos (como imágenes, por ejemplo) con el fin de poder ingresar a otros ordenadores.

4.2.1.4 Phishing. Se conoce como phishing a la práctica por medio de la cual los atacantes obtienen información personal e incluso confidencial a través del uso de sitios web que suplantan portales de confianza, como el de entidades bancarias, educativos, de salud e incluso gubernamentales. De acuerdo con LIA Solutions Colombia[27], un ataque tipo phishing inicia a través de un correo electrónico enviado a un usuario haciendo pasar por una entidad de confianza y solicitando información bajo algún tipo de pretexto, así como un enlace del supuesto sitio legítimo en el cual ingresar la información requerida.

Este tipo de ataques hacen uso del desconocimiento, falta de cultura en seguridad informática de las personas y el factor miedo mediante mensajes de bloqueo de cuentas, caducidad de información, entre otras cosas. Además del correo, el enlace es un factor fundamental puesto que dirige al usuario a un sitio que no es el real de la organización que se está suplantando pero que ha sido creado con tal nivel de detalle que una persona incauta pensará que está en el portal web de su entidad de confianza e ingresará datos tan delicados como su usuario, claves, número de cuenta, entre otros.

---

[25] PANDA SECURITY. (s.f.). *Virús informático*. Obtenido de PANDA SECURITY: http://www.pandasecurity.com/colombia/homeusers/security-info/classic-malware/virus

[26] MASADELANTE. (s.f.). *¿Qué es un virus informático?* Obtenido de Masadelante.com: http://www.masadelante.com/faqs/virus

[27] PANDA SECURITY. (s.f.). *Virús informático*. Obtenido de PANDA SECURITY: http://www.pandasecurity.com/colombia/homeusers/security-info/classic-malware/virus

De acuerdo con el sitio web infospyware.com[28], en el phishing se suele buscar la obtención de los siguientes datos:

- Datos personales.
- Direcciones de correo electrónico.
- Números de documentos de identidad.
- Datos de localización y contacto.
- Información financiera:
    - Números de tarjetas de crédito.
    - Números de cuentas.
    - Información de Home Banking o E-Commerce.
- Credenciales de acceso.
- Redes sociales.
- Cuentas de correo.

Por otro lado, se distinguen los siguientes como los principales medios de propagación[29]:

- Correo electrónico.
- Redes sociales.
- SMS\MMS (Mensajes vía teléfonos móviles).
- Llamadas telefónicas.
- Infección de programa maligno.

En general se puede detectar ciertos elementos que ayudan a reconocer un posible ataque de phishing, o, en otras palabras, a reconocer un correo y sitio web legítimo de uno que no lo es. Nuevamente, y de acuerdo la publicación de Infospyware, estos son los elementos para tener en cuenta:

- Para el caso de los correos:

    - El remitente del correo es desconocido o sospechoso (por ejemplo, el dominio del correo no concuerda con el dominio del sitio web legítimo,

[28] RIVERO, M. (s.f.). *¿Qué es el phishing?* Obtenido de Infospyware: https://www.infospyware.com/articulos/que-es-el-phishing/

[29] IDEM

incluso en algunos casos el correo ni siquiera está relacionado con la entidad que suplanta).

- El mensaje tiene muchos destinatarios, desconocidos en su gran mayoría.

- El asunto del mensaje no es claro, o no es común en el tipo de mensajes que el usuario podría recibir de la entidad suplantada (especialmente en aquellos casos en los cuales el usuario si tiene un vínculo con dicha entidad).

- Una de las características más importantes a analizar es el enlace que acompaña el correo que supuestamente lleva al sitio web de la entidad para el ingreso de los datos que se solicitan, y es que, aunque en el texto se pueda ver una dirección web legítima el enlace realmente lleva a una dirección totalmente diferente, lo cual se puede evidenciar en la barra de estado del navegador al poner el ratón sobre el enlace en cuestión.

- A diferencia de los correos legítimos, un intento de phishing dirige su correo de forma general, es decir, no utiliza el nombre del usuario sino únicamente palabras como señor, señora, cliente, etcétera.

- La mayoría de los correos relacionados con el phishing están llenos de mensajes alarmistas, como que la cuenta será cancelada o incluso que perderá X beneficio o dinero por no actualizar su información en la entidad.

- Finalmente, aunque no es una regla general, los errores de ortografía y gramática pueden estar incluidos en correos phishing.

- Los sitios web: Como se ha mencionado, el sitio web es hecho con un nivel de detalle que lo hace muy similar al portal web legítimo de una entidad, sin embargo, hay algunos elementos para tener en cuenta:

  - El sitio web no está en una plataforma segura y certificada, y no está usando el protocolo seguro: https.

  - La URL no coincide con la legítima de la entidad que se está intentando suplantar, tiene elementos extraños en la dirección y redirecciones.

  - Solicitan datos de autenticación que no son los habituales en el sitio web legítimos.

  - Los enlaces dentro del sitio web no coinciden con la dirección mostrada en la barra de estado del navegador (como ocurre en el correo). Esto es especialmente importante de verificar cuando se usan URL’s cortas.

4.2.1.5 Acceso no autorizado a la web. Cuando se usa la expresión WEB se hace referencia a todos los servicios que existen actualmente en la red, sean estos estáticos (HTML), dinámicos (PHP) o aplicaciones (java, .NET). De acuerdo con Andrés Figoli[30] "*El acceso no autorizado -aplicado en forma general-…a un sistema informático consiste en acceder de manera indebida, sin autorización o contra derecho a un sistema de tratamiento de la información con el fin de obtener una satisfacción de carácter intelectual por el desciframiento de los códigos de acceso o passwords, no causando daños inmediatos y tangibles en la víctima, o bien por la mera voluntad de curiosear o divertirse de su autor*".

Actualmente la información se ha convertido en un activo valioso para las organizaciones, y aunque inicialmente la definición de acceso no autorizado a un sistema informático fuera el de un intento de calmar la curiosidad, la realidad es que en los últimos tiempos se ha visto que estos ataques han pasado a ser un tema de poder e incluso de dinero. Casos como el de WikiLeaks[31] y la publicación de cantidades importantes de información o el caso de Ashley Madison[32] que estuvo rodeado de incidentes de chantajes y suicidios, demuestran cómo ha cambiado este interés lúdico o curiosidad y se ha pasado a otros niveles más serios.

Se distinguen métodos para el acceso a sistemas informáticos (incluidos los sitios web) como los siguientes[33]:

- Puertas falsas: puertas o accesos disponibles para la recuperación de información o del mismo sistema en caso de fallos.

---

[30] FIGOLI PACHECO, A. (s.f.). *El acceso no autorizado a sistemas informáticos*. Obtenido de Buscalegis: http://www.buscalegis.ufsc.br/revistas/files/anexos/2778-2772-1-PB.html

[31] AFP. (07 de 04 de 2013). *Wikileaks publica este lunes 1,7 millones de documentos diplomáticos*. Obtenido de El Espectador: http://www.elespectador.com/noticias/wikileaks/wikileaks-publica-lunes-17-milllones-de-documentos-dipl-articulo-414599

[32] INFOBAE. (24 de 08 de 2015). *Suicidios, chantajes y un mapa de infieles, entre las consecuencias del ataque a Ashley Madison*. Obtenido de Infobae: https://www.infobae.com/2015/08/24/1750447-suicidios-chantajes-y-un-mapa-infieles-las-consecuencias-del-ataque-ashley-madison/

[33] FIGOLI PACHECO, A. (s.f.). *El acceso no autorizado a sistemas informáticos*. Obtenido de Buscalegis: http://www.buscalegis.ufsc.br/revistas/files/anexos/2778-2772-1-PB.html

- Llaves maestras: software no autorizado para realizar acciones sobre un sistema informático o sobre archivos.

- Pinchado de líneas: intervención de los canales de transmisión de datos.

Para lograr o ejecutar estos métodos los atacantes se pueden valer de herramientas como[34]:

- Sniffers: encargados de interceptar información que circulan por la red.

- Rootkits: programa usado para eliminar o enmascarar los rastros dejados tras un ingreso no autorizado a un sistema.

- Troyan Horse.

- Gusanos y virus.

- Satan (Security Administrator Tool For Analysing Networks): programa para análisis de redes y detección de vulnerabilidades.

4.2.1.6 Robo de elementos críticos de hardware. Un sistema informático requiere de una base tecnológica física sobre la cual operar, esto implica el uso de servidores, sistemas de almacenamiento, equipos de redes, cableado, entre otros elementos. Tal como lo menciona el artículo "Seguridad Física de los Sistemas"[35] publicado por la Red Iris considera el "Hardware es frecuentemente el elemento más caro de todo sistema informático. Por tanto, las medidas encaminadas a asegurar su integridad son una parte importante de la seguridad física de cualquier organización". Uno de los principales problemas relacionados con el robo de elementos críticos está relacionado directamente con las facilidades en el acceso físico a los centros de datos donde los equipos se encuentran. Esto permite entre otras cosas:

- El hurto de elementos de almacenamiento (discos duros) con la consecuente pérdida de información.

---

[34] IDEM

[35] RED IRIS. (15 de 07 de 2002). *Seguridad física de los sistemas*. Obtenido de Red IRIS: https://www.rediris.es/cert/doc/unixsec/node7.html

- La pérdida de equipos completos (servidores).
- La pérdida de equipos de comunicaciones (enrutadores, conmutador, cableado).
- Robo de cableado.

En cualquiera de los casos la posibilidad de un mal funcionamiento de la estructura informática en general es latente y peligrosa. No obstante en este punto se ha hablado únicamente de los equipos de centros de datos (que deberían tener medidas de seguridad físicas como estar en un espacio cerrado y que además solo sean accesibles por personas estrictamente autorizadas) pero los de usuario final también corren riesgos (en general son los más vulnerables) dado que "mientras que parte de los equipos estarán bien protegidos, por ejemplo los servidores de un departamento o las máquinas de los despachos, otros muchos estarán en lugares de acceso semipúblico, como laboratorios de prácticas; es justamente sobre estos últimos sobre los que debemos extremar las precauciones"[36]. La pérdida de un equipo de un equipo de usuario final no solo genera problemas en cuanto a la operatividad de la organización, sino que también genera riesgo respecto a la información contenida en el dispositivo sino a las posibles configuraciones para el acceso a la red y otros recursos dentro de la organización.

Una situación de robo se puede presentar de diversas formas, desde el ingreso no autorizado y planeado de una persona al centro de datos evadiendo los sistemas de seguridad (si existen) hasta el hurto común dentro de las instalaciones abiertas al público o el robo a funcionarios que se desplazan con sus equipos fuera de la organización.

4.2.1.7 Ataques de aplicaciones web – Inyección de SQL. De acuerdo con OSWASP[37] Los ataques por inyección de SQL consisten en insertar código SQL a través de los campos de entrada en un formulario de una aplicación o una página web y de esa forma conseguir más información de la base de datos atacada. Mediante un ataque tipo Inyección de SQL se puede conseguir:

- Suplantar identidad.

---

[36] IDEM

[37] OWASP. (s.f.). *Inyección SQL*. Obtenido de OWASP: https://www.owasp.org/index.php/Inyecci%C3%B3n_SQL

- Alterar datos.
- Obtener datos privados.
- Destruir datos.
- Conseguir la administración del servidor de base de datos.

4.2.1.8 Ataque de aplicaciones web – Directory Transversal. En los ataques del tipo Directory Transversal el atacante busca llegar hasta directorios y archivos del servidor que están fuera de la estructura raíz de directorios del servidor web e incluso lograr la ejecución de comandos en el servidor[38].

Este tipo de ataques se basan en el uso los métodos GET y POST de las páginas web dinámicas (PHP, por ejemplo) en los cuales los atacantes cambian los parámetros (especialmente los relacionados con llamadas a contenidos y páginas de niveles inferiores) con el fin de buscar acceso a directorios más allá de la raíz de directorios web, como muestra el siguiente ejemplo:

Figura 7. Ejemplo de ataque tipo Directory Transversal

```
GET http://test.webarticles.com/show.asp?view=../../../../../Windows/system.ini HTTP/1.1
Host: test.webarticles.com
```

Fuente: (ACUNETIX, s.f.)

4.2.1.9 Negación del servicio. Los ataques de negación de servicio, de acuerdo con la definición brindada en Symantec[39], buscan que el acceso de los usuarios a un servidor o a los servicios que este ofrece, generando traumatismo bien sea en la operación de una o varias organizaciones, o el malestar en los usuarios y daño en la imagen de la organización que ofrece los servicios.

En este tipo de ataques se hace uso de aplicaciones por medio de los cuales se envían de forma masiva paquetes de datos y solicitudes de respuestas, de tal forma que el servidor se satura y no puede atender más peticiones y por tal razón no puede continuar

[38] ACUNETIX. (s.f.). *Directory Traversal Attacks*. Obtenido de Acunetix: https://www.acunetix.com/websitesecurity/directory-traversal/

[39] SYMANTEC. (s.f.). *Ataques DoS*. Obtenido de Glosario Symantec: https://www.symantec.com/es/mx/security_response/glossary/define.jsp?letter=d&word=dos-denial-of-service-attack

ofreciendo sus servicios. Este tipo de ataques son aplicables a cualquier servidor conectado a la red y su mayor fortaleza se encuentra en su simplicidad como en la posibilidad de hacerlo de forma distribuida, es decir, usando múltiples equipos desde diferentes ubicaciones (que han sido infectados o controlados mediante el uso de virus, gusanos y troyanos, por ejemplo) mediante herramientas como TFN, TFN2K y Trinoo. En años recientes empresas de gran envergadura han sufrido este tipo de ataques: Telegram en Julio del 2015[40], Facebook y Twitter en 2009, y otros casos que han sido reportados en los medios.

4.2.1.10 Ingeniería social. La ingeniería social es una modalidad de ataque que sirve de inicio para obtener objetivos mayores y que busca mediante el engaño, la suplantación, la manipulación y el desconocimiento de los usuarios acceder a información; en cierta forma está más enfocada en lo psicológico de los usuarios que en lo técnica, esto significa que se vale en gran medida de la curiosidad o incluso el morbo para ser más efectivo. De acuerdo con Montero Abujas[41], los ataques de ingeniería social se pueden dividir en las siguientes fases:

- Fase de Acercamiento: se busca ganar la confianza del usuario.
- Fase de Alerta: se busca alarmar al usuario y ver la forma en que responde ante la situación.
- Distracción: se distrae al usuario de la alerta, haciendo que se olvide y continúe con sus actividades normales.

[40] LOPEZ, M. (10 de 07 de 2015). *¡A cubierto! Telegram esta sufriendo un ataque DDoS a escala global*. Obtenido de Genbeta: https://www.genbeta.com/mensajeria-instantanea/a-cubierto-telegram-esta-sufriendo-un-ataque-ddos-a-escala-global

[41] MONTERO ABUJAS, D. (2017). *Ingeniería social.* Obtenido de Slideshare: https://es.slideshare.net/monteseugenio/owand11-granada-ingeniera-social

Un atacante que use la ingeniería social se puede valer de varios métodos para lograr su objetivo[42] [43] [44] [45]:

- Pretexting: esta relacionado con simular o hacerse pasar por otras personas (por ejemplo, suplantando a una autoridad local o un ejecutivo de una entidad bancaria) para obtener información privada

- Phishing: Consiste en el engaño por medio del correo electrónico y la suplantación de identidad, específicamente haciéndose pasar por un banco o entidad de reconocimiento, solicitando información privada, adjuntando archivos maliciosos o dirigiendo a sitios web falsos.

- Smishing: En este caso el engaño se realiza mediante mensajes de texto o SMS, los cuales contienen enlaces maliciosos

- Vishing: es parecido al phishing, pero hace uso del medio telefónico para obtener información del usuario, suplantando por ejemplo un IVR de una entidad bancaria.

- Baiting: Utilizando la curiosidad el atacante logra su objetivo, para lograrlo deja un elemento o dispositivo "abandonado", en general un elemento de almacenamiento que el usuario incauto llevará a su ordenador e intentará abrir sin darse cuenta de que el elemento tiene software malicioso que se introduce en el computador.

- Dumpster Diving o Trashing: búsqueda de información en la basura, como documentos, agendas, notas, discos ópticos.

---

[42] BRICENO, E. (25 de 04 de 2012). *Guía de la semana: Qué es la ingeniería social y como estar prevenidos.* Obtenido de Hipertextual: https://hipertextual.com/archivo/2012/04/que-es-la-ingenieria-social-y-como-estar-prevenidos/

[43] SANDOVAL CASTELLANOS, E. J. (s.f.). *Ingeniería social: corrompiendo la mente humana*. Obtenido de Revista Seguridad: http://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana

[44] LISA INSTITUTE. (08 de 05 de 2020). *Guía práctica contra la ingeniería social*. Obtenido de LISAINSTITUTE.COM: https://www.lisainstitute.com/blogs/blog/guia-practica-ingenieria-social

[45] AVAST ACADEMY TEAM. (19 de 05 de 2020). *Ingeniería Social*. Obtenido de AVAST.COM: https://www.avast.com/es-es/c-social-engineering

4.2.2 Normas y estándares. De acuerdo con la página web Deconceptos.com[46] se define estándar como “modelo, norma o regla o patrón a seguir” y a continuación indica que “Los estándares son construcciones culturales efectuadas por quienes poseen autoridad ética, técnica, teórica o científica, según sea el caso, de público conocimiento que nos dan confianza en nuestro accionar, pues nos sirven de guía y referencia; y a posteriori permite controlar lo producido para realizar sobre ello un juicio de valor”.

Se considera entonces que un estándar es un conjunto de reglas, normas, procedimientos, en general una guía que permite a las organizaciones replicar una serie de acciones en sus departamentos o procesos. Es importante señalar que un estándar debe ser aceptado y establecido por un consenso de entidades de relevancia para el área en el cual se va a aplicar, en las cuales se pueden incluir entidades privadas del sector o entidades gubernamentales y de control, puesto que “estos –los estándares – implican obtener el consenso entre grupos heterogéneos, multidisciplinarios y ante todos antagónicos, los cuales son útiles en la medida en que sean adoptados por una amplia variedad de organizaciones”[47] de acuerdo a lo expresado por el ICDE sobre los estándares, que señala además:

> “*La estandarización persigue fundamentalmente tres objetivos:*
>
> - *Simplificación: Se trata de reducir los modelos quedándose únicamente con los más necesarios.*
> - *Unificación: para permitir el intercambio de un nivel determinado.*
> - *Especificación: se persigue evitar errores de identificación creando un lenguaje claro y preciso.*"[48].

Lo anterior implica que un estándar busca brindar pautas y buenas prácticas para llevar a cabo procesos más efectivos y claros, mejor documentados, ordenados teniendo como

---

[46] DE CONCEPTOS. (s.f.). *Concepto de estándar*. Obtenido de De Conceptos: http://deconceptos.com/ciencias-sociales/estandar

[47] ICDE. (s.f.). *Estándares*. Obtenido de Infraestructura Colombiana de datos espaciales: http://www.icde.org.co/web/guest/wiki/-wiki/Wiki%20de%20la%20ICDE/Estándares

[48] IDEM

base la experiencia previa de otras organizaciones y mejorando la imagen de la empresa, así como facilitar la implementación de nuevos procesos dentro de la misma.

En general en las organizaciones se pueden encontrar varios tipos de estándar aplicados y conviviendo, y es que los estándares se pueden llevar a cualquier área de una organización, ya sea de forma general como los estándares de calidad (ISO 9000) que son aplicables a cualquier parte de una empresa, sea esta contable, gestión humana, sistemas, etcétera o por otro lado tener estándares enfocados a temas más puntuales, ya sean estos de seguridad de la información (ISO 27000), gestión de TI (ITIL[49]), contabilidad (NIF), entre otros. Y es que existen diferentes normas y estándares que se pueden aplicar en las organizaciones como lo menciona el sitio web pdcahome.com en su artículo Las normas ISO más usadas[50] en el que entrega un listado de normas ISO de diferente naturaleza y que son consideradas como las de uso común en diferentes ámbitos.

En relación con el área de TI los estándares describen las tareas y la manera como se usan los recursos tecnológicos y la información, las buenas prácticas en desarrollo de software, entre otros aspectos. Algunos de los estándares relacionados con TI son los siguientes[51]:

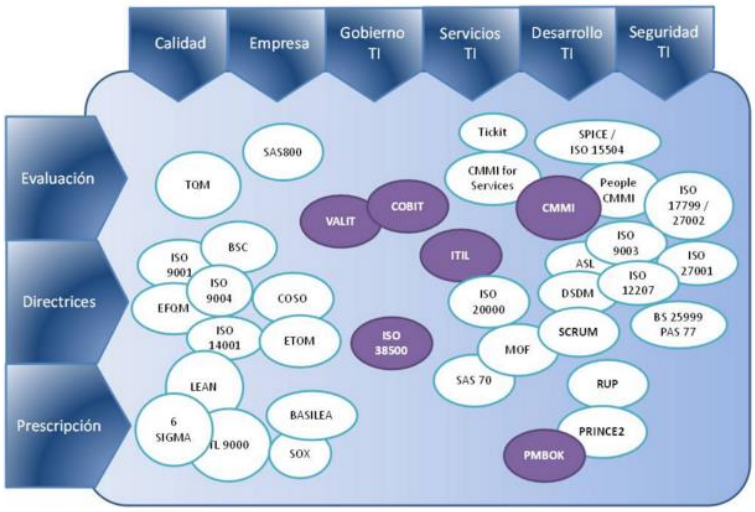
- CRAMM.
- COBIT.
- ITIL.
- OCTAVE.
- RISK IT.
- MAGERIT.

[49] ALMUNIA, P. (s.f.). *IEDGE - Estándares para la gestión de TI*. Obtenido de IEDGE Business School: https://www.iedge.eu/pablo-almunia-estandares-para-la-gestion-de-ti-primera-parte#comment-1736

[50] PDCAHOME. (27 de 03 de 2013). *Las normas ISO más usadas*. Obtenido de https://www.pdcahome.com/4168/las-normas-iso-mas-usadas/

[51] ALMUNIA, P. (s.f.). *IEDGE - Estándares para la gestión de TI*. Obtenido de IEDGE Business School: https://www.iedge.eu/pablo-almunia-estandares-para-la-gestion-de-ti-primera-parte#comment-1736

Figura 8. Estándares relacionados con TI



Fuente: (ALMUNIA, s.f.)

4.2.2.1 CRAM no consiste puntualmente en un estándar, pero si en una metodología enfocada en el análisis de riesgos, e incluso se considera como una herramienta por medio de la cual se identifican las posibles amenazas y probables eventos indeseados que se puedan producir contra el sistema o la infraestructura de la organización. Esta metodología ha sido desarrollada por la CCTA de Inglaterra desde el año 1987, y "el significado del acrónimo proviene de CCTA Risk Analysis and Management Method"[52].

La metodología CRAMM busca proteger la confidencialidad, integridad y disponibilidad de la información, un concepto que se repite constantemente en los sistemas de gestión de seguridad de la información y es que incluso esta metodología y sus herramientas son compatibles con ISO 27000.

CRAMM no es una metodología para aplicar en una etapa específica del sistema puesto que puede hacer parte de diferentes fases del ciclo de vida de un SI, y en general es aplicable a cualquier sistema de información. En resumen, la metodología CRAMM se puede aplicar en las siguientes fases[53]:

[52] SEGURIDAD INFORMÁTICA UFPS. (s.f.). *Herramienta de evaluación de riesgo - CRAMM*. Obtenido de SEGURIDAD INFORMÁTICA UFPS: https://seguridadinformaticaufps.wikispaces.com/Herramienta+de+Evaluacion+de+Riesgo-CRAMM

[53] IDEM

- En la etapa de planificación.
- En la etapa de estudio de factibilidad.
- En la etapa del análisis de negocio.
- Antes, durante y después de la ejecución del proyecto o sistema.

La metodología CRAMM se enfoca en tres fases[54]:

- Identificación y valoración de activos o establecimiento de objetivos de seguridad: En esta etapa se identifican los activos de la organización, pudiendo ser estos de naturalezas diferentes, por ejemplo, hardware, software, fuentes de datos, infraestructura, entre otros.

  En esta etapa también se les da valor a los activos de acuerdo con su costo de reemplazo, es decir, cuánto cuesta recuperar el activo en caso de pérdida de este, ya sea un servidor o la información contenida en una base de datos.

- Evaluación de riesgos y amenazas: después de tener identificados los activos y su valor en la organización es importante conocer el nivel de riesgo al que se encuentran expuestos, esto quiere decir:

  - El tipo y nivel de las amenazas que pueden afectar al sistema.

  - Evaluar el grado de vulnerabilidad del sistema frente a dichas amenazas.

  - Combinar amenazas, vulnerabilidad y activos para determinar el nivel de riesgo.

- La tercera fase nace del análisis de las dos anteriores y corresponde con las contramedidas y recomendaciones a seguir para minimizar los riesgos y los efectos que la materialización de estos pueda tener sobre el sistema estudiado. CRAMM ya cuenta con una importante cantidad de contramedidas preestablecidas (y se pueden agregar las que la propia organización considere oportuno incluir).

[54] MARQUIS, H. (17 de 12 de 2008). *10 Steps to Do It Yourself CRAMM.* Obtenido de ITSM Solutions: http://www.itsmsolutions.com/newsletters/DITYvol4iss50.pdf

4.2.2.2 COBIT De acuerdo con el Blog Seguridad de la información en Colombia[55] COBIT es presentado por ISACA como un conjunto de mejores prácticas para el manejo de la información que ha evolucionado desde el año 1996 (Cobit 1) enfocado en los procesos de auditoría informática, pasando por los procesos de control, Administración, Gobierno de IT y terminando en la versión actual, COBIT 5 dirigido al Gobierno Empresarial de TI.

En general se puede considerar que COBIT es una guía para poder obtener el mejor valor de TI y una administración óptima de la información y de los recursos tecnológicos y establecer. La idea detrás de COBIT es constituir a TI como un apoyo para la organización de tal manera que le permita alcanzar sus objetivos y la gestión de sus necesidades, ayudando en la toma de decisiones y llevando un control del cumplimiento de objetivos.

COBIT (y en especial la última versión) se basan en un esquema de 5 principios y 7 habilitadores descritos por Melisa Osores en el sitio web de TechTarget[56]:

- Principios
    - Satisfacer las necesidades de los interesados: alrededor de una organización existen diferentes grupos de personas con intereses puestos en la empresa, como los socios, inversionistas, empleados o los clientes de la organización. En este sentido estos intereses son importantes y por tal razón los objetivos empresariales y los de TI deben estar vinculados y alineados.
    - Cubrir la empresa de extremo a extremo: El cambio de visión de las organizaciones, aunque no es suficiente sí que ha sido significativo, puesto que se sigue el camino de considerar al departamento de TI como un activo y no como un costo (especialmente cuando de seguridad de la información se trata). Para el grupo directivo TI debe hacer parte de sus intereses y del conjunto completo que es la empresa e integrar el gobierno empresarial de TI con el gobierno organizativo.

---

[55] MARQUIS, H. (17 de 12 de 2008). *10 Steps to Do It Yourself CRAMM.* Obtenido de ITSM Solutions: http://www.itsmsolutions.com/newsletters/DITYvol4iss50.pdf

[56] OSORES, M. (07 de 2014). *Principios de COBIT 5 para el gobierno efectivo de TI.* Obtenido de Techtarget: https://searchdatacenter.techtarget.com/es/cronica/Principios-de-COBIT-5-para-el-gobierno-efectivo-de-TI

- Aplicar un solo marco integrado: Existen en el mercado diferentes marcos y estándares relacionados con TI y con la gestión empresarial. COBIT está alineado con ellos y actúa como un marco integrador de gobierno y administración de TI.

- Habilitar un enfoque holístico: cuando se habla del concepto de la holística se parte del concepto de analizar o entender los eventos teniendo en cuenta el contexto y los protagonistas de este, así como las múltiples interacciones entre ellos y no como una situación aislada. Esto se debe trasladar al gobierno de TI con el fin de tener en cuenta todos los componentes.

- Separar el gobierno de la administración: cuando se habla de gobierno se hace referencia enfocada la junta directiva y buscan que los objetivos de la organización se alcancen mediante una serie de acciones, evaluaciones y monitoreo. Por su parte la administración está bajo el liderazgo del CEO para planear, crear, realizar y monitorear las actividades de tal forma que estén alineadas con lo que la dirección ha establecido.

- Procesos Habilitadores: se puede definir los procesos habilitadores como los factores que de manera individual o colectiva influyen en el éxito o fracaso del gobierno de TI y la gestión de la empresa. Son elementos o conceptos que ayudan a que las políticas y procedimientos se desarrollen de forma más efectiva. COBIT 5 entrega los siguientes procesos habilitadores[57]:

    - Principios, políticas y marcos de trabajo: guías para la gestión del día a día en la organización.

    - Procesos: Son las actividades que se llevan a cabo para alcanzar los objetivos de TI.

    - Estructura Organizacional: Corresponde con las áreas de la organización involucradas en la toma de decisiones.

    - Cultura, ética y comportamiento: está relacionado con los individuos dentro de la organización y su relación y efecto en el éxito de la organización.

[57] CHAUI. (15 de 05 de 2015). *Cobit 5 - Fundamentación de facilitadores / habilitadores / catalizadores.* Obtenido de Chaui201511700911004: https://chaui201511700911004.wordpress.com/2015/05/15/cobit-5-fundamentacion-de-facilitadores-habilitadores-catalizadores/

- Información: como se ha mencionado, uno de los activos más valiosos de las organizaciones hoy en día, usada y utilizada por toda la organización en la toma de decisiones.

- Servicios, infraestructuras y aplicaciones: como su nombre lo indica, hace referencia a la infraestructura, tecnología y servicios que la empresa usa para sus actividades.

- Personas, habilidades y competencias: este último ítem hace referencia al recurso humano de la organización, importante como cualquiera de los habilitadores anteriores para el éxito de los procesos y el cumplimiento de los objetivos.

4.2.2.3 ITIL. En relación con los Servicios Informáticos desde 1980 se ha desarrollado un estándar mundial conocido como Biblioteca de Infraestructura de Tecnologías de la Información (Conocida por sus siglas en inglés como ITIL)[58], la cual entre sus puntos a favor se encuentra con una amplia aplicación en diferentes tipos de empresas además de ser de libre utilización. ITIL se basa en el concepto de TI como un proveedor de servicios informáticos de calidad para el cliente que cumpla y se corresponda o cumpla con los objetivos del negocio.

ITIL se puede describir como una serie de documentos que apoyan en la gestión de TI y alineados con la Norma ISO 20000. Los documentos se encuentran divididos en los siguientes libros[59]:

- Estrategia del servicio.
- Diseño del Servicio.
- Transición del Servicio.
- Operación del Servicio.
- Mejora Continua del Servicio.

---

[58] OSIATIS. (s.f.). *¿Qué es ITIL?* Obtenido de OSIATIS: http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/fundamentos_de_la_gestion_TI/que_es_ITIL/que_es_ITIL.php

[59] ITIL BOOKS. (s.f.). *How is ITIL organized.* Obtenido de ITIL Training academy: http://www.itil.org.uk/how.htm

4.2.2.4 OCTAVE. Octave está relacionado con la gestión de riesgos y se presenta como una técnica de planificación y consultoría en Seguridad enfocado en los temas relacionados con la estrategia y la práctica. El método OCTAVE se basa inicialmente en tres fases[60]:

- Identificación de la información a nivel gerencial.
- Identificación de la información a nivel operacional.
- Identificación de la información a nivel de usuario final.

A partir de las fases anteriores se desprenden otros 5 puntos:

- Consolidación de la información y creación de perfiles de amenazas.
- Identificación de componentes claves.
- Evaluación de componentes seleccionados.
- Análisis de riesgos de los recursos críticos.
- Desarrollo de estrategias de protección.

Sin embargo, es importante tener en cuenta que no existe una única forma de "implementar" OCTAVE en una organización, sino que hay 3 métodos[61]:

- Método Octave: enfocado en organizaciones de 300 o más empleados, con jerarquía de múltiples capas e infraestructura tecnológica propia y herramientas propias de evaluación de vulnerabilidad e interpretación de resultados. Esta metodología usa entonces tres fases:
    - Identificación de elementos críticos y las amenazas sobre ellos.
    - Identificación de vulnerabilidades.
    - Desarrollo de una estrategia basada en prácticas y planes de mitigación de riesgos.

- Método Octave-S: Enfocado en organizaciones más pequeñas (100 personas o menos), cumple los mismos criterios del método Octave, pero se ajusta a las

[60] DUQUE OCHOA, B. R. (s.f.). *Metodologías de gestión de riesgos (OCTAVE, MAGERIT, DAFP).* Obtenido de AuditoriaUC20102mivi: http://auditoriauc20102mivi.wikispaces.com/file/view/Metodolog%C3%ACas+deGesti%C3%B2n+de+Riesgos.pdf

[61] IDEM

restricciones y recursos limitados de las pequeñas empresas mediante procesos más simples y una documentación (formatos) diferentes.

- Método Octave-Allegro: Variante del método Octave centrado en los activos de la información (el resto de los activos se evalúan en relación con la información).

4.2.2.5 MAGERIT. MAGERIT corresponde con un marco de trabajo enfocado en la gestión del riesgo, en este caso se trata de la implementación del proceso de gestión de riesgos. MAGERIT presenta los siguientes objetivos[62]:

- Crear conciencia en los responsables de la organización sobre los riesgos y la necesidad de gestionarlos.
- Ofrecer un método para el análisis de los riesgos.
- Ayudar en la gestión y control de los riesgos.
- Preparar la organización para procesos de auditoría, certificación y similares.

En la búsqueda de cumplir con dichos objetivos MAGERIT se basa en los siguientes informes o documentos:

- Modelo de valor: representación del valor de los activos para la organización.

- Mapa de riesgos: relación de amenazas y activos.

- Declaración de aplicabilidad: evaluación de la aplicabilidad de un conjunto de salvaguardas en el sistema.

- Evaluación de salvaguardas: Evaluación de la efectividad de las salvaguardas.

- Estado de riesgo: después de aplicadas las salvaguardas, cual es el estado de riesgo (residual).

- Informe de insuficiencias: después de aplicadas las salvaguardas se analiza en qué casos no son suficientes.

- Cumplimiento de normativas: evaluación de conformidad respecto a una normativa.

---

[62] IDEM

- Plan de seguridad: aplicación de las salvaguardas para el tratamiento de riesgos.

4.2.2.6 ISO 27000. ISO 27000 es quizás una de las normativas más conocidas en el mundo de TI, especialmente porque está enfocada en el que se ha convertido en el recurso más valioso para las empresas actuales: La Información. El origen de la norma 27000 se encuentra en la *International Organization of Standarization* (ISO) en el año 2005 pero nace realmente a partir de la evolución de otros estándares previos, a partir de las normas establecidas por la *British Standars Institution* (BSI) en los años 1900 (BS 5750 en el año 1979 que dio origen a ISO 9001; BS 7750 en 1992 pasaría posteriormente a ser ISO 14001, BS 8800 de 1996 que se convirtió en OHSAS 18001), especialmente a finales de los años 90's cuando se establecieron las normas BS 7799-1 (año 1995) con las mejores prácticas para la seguridad de la información, que a su vez recibieron las respectivas revisiones (BS 7799-1:1999; BS 7799-2:1999; BS 7799-2:2000).

En el año 2000 ISO tomo la norma como base para la ISO\IEC 17799:200 que mantuvo mucho del estándar británico para posteriormente en el año 2005 realizar la primera revisión de la norma (ISO\IEC 17799:2005) y al tiempo dar origen a la ISO\IEC 27001 (ISO\IEC 27001:2005). Sería en 2007 cuando ISO\IEC 17799 pasaría a ser transformada en lo que hoy conocemos como ISO\IEC 27002:2005, para finalmente llegar a la versión del año 2013 (ISO\IEC 27001:2013). Es importante señalar que si bien estas normas se aplican a muchas empresas estas no son gratuitas o de libre difusión, deben ser compradas y están protegidas por derechos de autor, igualmente se debe pagar por el proceso de certificación que garantizará que la organización cumple y puede obtener y presentar su certificado como parte de su documentación.

La serie ISO\IEC 27000 corresponde a un conjunto de estándares relacionado con los Sistemas de Gestión de Seguridad de la Información y está compuesto por diferentes siguientes estándares y documentos[63]:

- **Estándares de la IOS\IEC 27000:**
    - ISO\IEC 27001: Contiene los requisitos para la implantación del SGSI dentro de la organización con un enfoque en la gestión de riesgos y mejora continua de los procesos (algo que suele repetirse con las diferentes

[63] ISO 27000. (2005). *ISO 27000.* Obtenido de ISO270000.ES: http://www.iso27000.es/iso27000.html

normas ISO\IEC). Podría considerarse como la parte fundamental y base de todo el conjunto ISO 27000.

- ISO\IEC 27002: El código de buenas prácticas de la norma ISO\IEC 27000.
- ISO\IEC 27003: Constituye un apoyo a la ISO\IEC 27001, siendo una especie de guía o conjunto de directrices para implementar un SGSI.
- ISO\IEC 27004: Esta parte de la norma corresponde a métricas que se deberían usar en la gestión de la seguridad de la información.
- ISO\IEC 27005: La evaluación de riesgos ese el tema principal de este parte de la norma ISO\IEC 27000.
- ISO\IEC 27006: Está enfocada en las entidades que certifican otras organizaciones en ISO\IEC 27000.
- ISO\IEC 27007: Corresponde a la guía para realizar auditorías de ISO\IEC 27000.
- ISO\IEC 27008: Guía de auditoría para los controles seleccionados para el SGSI.
- ISO\IEC 27009: Se encuentra en desarrollo, enfocada en el sector de servicios específicos.
- ISO\IEC 27010: Guía para la gestión de un SGSI en los cuales la información se comparte entre organizaciones o sectores.
- ISO\IEC 27011: Guía de interpretación de implementación y gestión del SGSI en organizaciones del sector de las telecomunicaciones.
- ISO\IEC 27013: Guía de implementación integrada de ISO\IEC 27001:2005 y de ISO\IEC 20000-1.
- ISO\IEC 27014: Guía de gobierno corporativo de la seguridad de la información.
- ISO\IEC TR 27015: Guía de implementación de SGSI para entidades del sector financiero y seguros.
- ISO\IEC TR 27016: Guía de valoración de los aspectos financieros de la seguridad de la información.

- ISO\IEC 27018: Código de buenas prácticas en entornos de cloud-computing.
- ISO\IEC TR 27019: Guía para los sistemas de control específicos en el sector energético.
- ISO\IEC 27031: Guía para la adecuación de tecnologías de información y comunicación para la continuidad del negocio.
- ISO\IEC 27032: Relacionado con la seguridad informática, incluido redes, seguridad en Internet, infraestructuras críticas.
- ISO\IEC 27033: Esta parte de la norma está enfocado en redes.
- ISO\IEC 27034: Se enfoca en la seguridad en aplicaciones informáticas.
- ISO\IEC 27035: Guía sobre la gestión de incidentes de seguridad.
- ISO\IEC 27036: Guía relacionada con la seguridad con proveedores.
- ISO\IEC 27037: Directrices para las actividades relacionadas con la identificación, recopilación, consolidación y preservación de evidencias digitales de equipos móviles, tarjetas de memoria, cámaras y otros elementos electrónicos personales.
- ISO\IEC 27038: Relacionado con la seguridad en la redacción digital.
- ISO\IEC 27039: Relacionado con los sistemas de detección y prevención de intrusos.
- ISO\IEC 27040: Guía para la seguridad en medios de almacenamiento.
- ISO\IEC 27041: Guía relacionado con los métodos de investigación.
- ISO \IEC 27042: Directrices para el análisis e interpretación de evidencias digitales.
- ISO\IEC 27043: Principios y procesos de investigación para la recopilación de evidencias digitales.
- ISO\IEC 27044: Enfocado en la gestión de eventos y de seguridad de la información.
- ISO \IEC 27799: es la parte de la norma que está enfocada en el sector salud.

4.2.2.7 Metodología PDCA. Existen varias metodologías para la gestión de proyectos, por medio de las cuales se da un orden a las acciones que se realizan en pro de conseguir los objetivos de la manera más eficiente y directa. Dentro de las metodologías de proyectos que se suelen mencionar se encuentran[64]:

- Metodología del diagrama de Gantt: considerado como un método simple y efectivo, adecuado para personas que se están introduciendo en la gestión de proyectos.

- Pert\CPM: Una técnica que puede ser usada con Diagrama de Gantt.

- Método de la cadena crítica: método especialmente enfocado en proyectos complejo, con muy buenos resultados.

No obstante, en sistemas de gestión, como el de calidad (ISO 9000) o el de seguridad de la información (27001), se utiliza con mucha frecuencia (además de ser impulsado por los mismos estándares) el ciclo PDCA[65] o de Mejora Continua como también se le conoce y que hace referencia a cuatro palabras "claves":

- Planear (Plan): Consiste en preparar o definir qué es lo que se quiere lograr y como llegar a ese punto.

- Hacer (Do): Cuando ya se tiene claro el que y el cómo, el siguiente paso consiste en hacer lo que se ha planeado.

- Revisar (Check): no basta con realizar acciones, es importante verificar que lo hecho tiene el efecto buscado, verificar que se logran los objetivos planteados.

- Actuar (Act): ¿Que sucede cuando en la revisión se detectan problemas?, bueno la respuesta es hacer frente a esa situación, actuar frente a lo detectado y realizar

[64] OBS Business School. (s.f.). *Las 3 metodologías para la gestión de proyectos que más se utilizan*. Obtenido de OBS Business School: https://www.obs-edu.com/int/blog-project-management/administracion-de-proyectos/las-3-metodologias-para-la-gestion-de-proyectos-que-mas-se-utilizan

[65] CALIDAD & GESTIÓN. (s.f.). *Ciclo PDCA - Estrategía para la mejora continua*. Obtenido de Calidad & Gestión: http://www.calidad-gestion.com.ar/boletin/58_ciclo_pdca_estrategia_para_mejora_continua.html

cambios. Al ser un sistema cíclico, se vuelve al punto de planeación y se repiten los pasos.

En general, cuando se habla de sistemas de gestión, este sistema creado por el Dr. Williams Edwards Deming (del cual se deriva otro nombre con el que se conoce a PDCA, el Círculo de Deming) es bastante usado, pues resulta ser muy efectivo, dividiendo el proceso de implementación de una forma similar a la que se presenta a continuación:

- Planear:
    - Definir los objetivos de la organización respecto al sistema que se está implantando.
    - Establecer los procesos necesarios para llegar a esos objetivos.
    - Identificar situaciones de peligro o riesgo, vulnerabilidades.
    - Identificar elementos legales, regulaciones, entre otros, que puedan influir en el sistema.
    - Definir medidas de control.
- Hacer:
    - Implementar los procesos.
    - Asignar los recursos, definir responsables.
    - Comunicar las decisiones, procesos.
    - Capacitar.
- Control:
    - Realizar seguimiento a los procesos.
    - Recolectar y analizar datos de control.
    - Comparar con objetivos.
    - Documentar conclusiones.
    - Revisión de incidentes.

- Realizar auditorías internas\externas.
- Implementar acciones correctivas y preventivas.

- Actuar:
  - Revisión por parte de la dirección de los resultados de la etapa de control.
  - Modificar los procesos cuando sea necesario.
  - Mejorar el sistema.
  - Documentar los cambios.

4.3 MARCO CONCEPTUAL

El marco conceptual presenta las variables y conceptos importantes para el proyecto[66].

4.3.1 Información. El concepto de información se puede separar en conceptos más básicos que se van uniendo hasta crear el significado completo.

- Dato: Se entiende como dato a la unidad básica o mínima de la información, carente de significado por sí solo. Un dato puede ser un número, una letra, un píxel, entre otros. Un conjunto de estos elementos también pueden ser un dato, ejemplo 9873204, sin embargo, por sí mismo no dice mucho, pues no se puede

[66] DIP, P. (13 de 04 de 2008). *Dato e información*. Obtenido de Tecnología e Informática: http://latecnologiavirtual.blogspot.com/2008/04/dato-e-informacin.html

ISO TOOLS Excellence. (01 de 02 de 2018). *Los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad*. Obtenido de SGSI Blog especializado en Sistemas de Gestión de Seguridad de la Información: https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/

ISO27000.ES. (s.f.). *Glosario*. Obtenido de ISO27000.ES: http://www.iso27000.es/glosario.html

LORENZO PÉREZ, A. (26 de 06 de 2018). *Riesgo, amenaza y vulnerabilidad*. Obtenido de EQ2B Consulting: https://eq2b.com/riesgo-amenaza-y-vulnerabilidad-iso-27001/

saber si es una cifra (9’873.205 habitantes de una ciudad), un valor ($9’873.204), un número de identificación (CC. 9.873.204), entre otros.

- Información: Cuando un conjunto de datos es procesados, ordenados y se les da un valor o significado, se habla de información. En una empresa una base de datos contiene información, registros con un significado que permiten tomar decisiones.

- Fuente: Origen de la información (o del dato).

- Confidencialidad: Propiedad de la información en la cual la información solo está disponible o es accesible por su propietario o por quien este designe (autorice).

- Integridad: La integridad se refiere a la propiedad por medio de la cual la información se mantiene sin alteraciones accidentales o no autorizadas.

- Disponibilidad: Hace referencia a que la información se mantiene accesible y operativa (especialmente al hacer referencia sobre sistemas) para los usuarios autorizados.

4.3.2 Seguridad de la Información: Acciones por medio de las cuales se preservan los tres pilares de la información: confidencialidad, integridad y disponibilidad.

4.3.3 Vulnerabilidad: Hace referencia a las debilidades de un sistema, un activo, un proceso, control, etcétera, que puede ser aprovechado por una amenaza.

4.3.4 Amenaza: Se refiere a la causa u origen de un incidente capaz de provocar daños en los activos, sistemas, entre otros.

4.3.5 Riesgo: El riesgo es la posibilidad que la amenaza se materialice a través de una vulnerabilidad.

4.3.6 Impacto: Considerando la vulnerabilidad, si esta es explotada genera un coste (en términos económicos, operativos, etcétera) para la organización. Este coste se conoce como impacto.

4.3.7 Incidente: son los eventos inesperados o indeseados, (o evento) relacionados con la seguridad de la información (aunque abarca muchas otras situaciones), que ponen el riesgo o comprometen la seguridad de la información.

4.3.8 Tratamiento del riesgo: Las acciones que se realizan con el fin de disminuir o dar un controlar el riesgo.

4.3.9 Valoración del riesgo: situación en la cual se da un valor específico al riesgo detectado de acuerdo con el impacto que pueda generar, las vulnerabilidades asociadas, entre otros.

4.3.10 Control: Los controles abarcan todos los medios implementados con el fin de disminuir el nivel de riesgo (o riesgos) en la organización. Abarca procesos, políticas, procedimientos, entre otros.

4.3.11 Política: La política se puede interpretar como un instructivo mediante el cual los usuarios identifican las prácticas y procedimientos que la organización dispone para preservar la seguridad de la información.

4.3.12 Procedimiento: Conjunto de actividades por medio de las cuales se llega a un objetivo.

4.3.13 Activo: Cualquier elemento relacionado con el tratamiento de la información, incluida la misma información, los actores que interactúan con ella y los elementos donde es almacenada.

4.4 MARCO LEGAL

4.4.1 Panorama sobre la legislación de delitos informáticos. Tecnología es un término que se viene usando desde hace ya una importante cantidad de años, sin embargo, los temas de seguridad relacionados con este término apenas vienen madurando, están estabilizándose en el transcurso que se van presentando las necesidades. No obstante, la legislación informática en Colombia se enfrenta a varios problemas, entre ellos dos muy significativos que han regido el curso de las leyes en las tecnologías de la información desde el comienzo:

Primero, y partiendo desde el ámbito local, Colombia aún no está realmente preparado ni es independiente al momento de establecer sus políticas en cuanto a TI, esto significa que generalmente toma su base a partir de las leyes que otros países “pioneros” generan para superar sus problemas, o incluso, se acogen a las reglas de otras naciones para

legislar (tanto en TI como en otros campos) de tal forma que sean “acordes” para los tratados de libre comercio que se firman con naciones como EEUU, China, etcétera.

El segundo problema está directamente relacionado con el primero, y es que en la mayoría de los países de los cuales Colombia basa sus leyes informáticas están altamente saturados por las conveniencias de grandes empresas que influenciadas en tres sentidos: No aceptan la evolución de la tecnología, evolucionan con la tecnología a un paso muy lento o son punteros en la innovación y acomodan las reglas para su beneficio. Esto implica que se vean regulaciones que poco benefician a los usuarios de IT o simplemente van en contravía con la evolución de la Internet, por poner un ejemplo. Superado lo que vendría a ser como la fuente de las legislaciones informáticas en Colombia, se considera ahora lo que es la situación del país en este ámbito. Dentro de los primeros indicios sobre este tipo de legislación se encuentran las primeras leyes de derechos de autor[67]. Lastimosamente los derechos de autor se han convertido en un cáncer en la actualidad, limitando lo que en un principio parece quería fomentar: la innovación. La razón es simple, las grandes empresas parecen negociar en esta “nueva moneda”, demandando en todo lo que pueden y sienten que tienen derechos por una patente, aun cuando sea la común forma cuadrada de un teléfono celular.

Continuando con los 80’s, en el año 87 se regulan las escuchas telefónicas y un año más tarde se crea la Ley de Protección de Datos, la cual con el avance del tiempo ha cobrado cada vez más importancia protegiendo y devolviendo el control a los verdaderos propietarios de los datos personales: los usuarios a los cuales pertenecen esos datos, y evitando que las empresas abusen de la información personal. No obstante, y a pesar de los años que han pasado desde que se promulgara esta primera versión de la ley, es un hecho que la ciudadanía en general no tiene el conocimiento suficiente sobre estas leyes para hacer valer sus derechos correctamente. Años después, en 1998 se establecen las leyes que regulan el acceso y el uso del comercio electrónico[68], uno de los pasos que hicieron notar el avance que se ha presentado en relación a la tecnología de la información en el país, aun cuando en la actualidad las personas mantengan el temor al comercio electrónico (alimentado a su vez por las considerables noticias de “hackers” y

[67] CONGRESO DE LA REPUBLICA. (28 de 01 de 1982). *Ley 23 del 28 de Enero de 1982 sobre derecho de autor.* Obtenido de CONGRESO DE LA REPÚBLICA: http://www.informatica-juridica.com/anexos/Ley_23_28_enero_1982_derecho_autor.asp

[68] CONGRESO DE LA REPÚBLICA. (21 de 04 de 1998). *Proyecto de Ley No. 227*. Obtenido de Informática Jurídica: http://www.informatica-juridica.com/anexos/Proyecto_Ley_N%C2%BA_227_Abril_21_1998_Comercio_Electronico.asp

de fraude electrónico alimentado muchas veces más por las estafas que por reales ataques informáticos a sistemas comerciales).

En los años siguientes se han producido cambios en la legislación incluyendo la Ley 679 del 3 de agosto de 2001 que busca proteger a los menores de edad del abuso y la pornografía, y es que claro, existen iniciativas que realmente buscan el beneficio de los ciudadanos, incluidos los más pequeños. El ámbito laboral tampoco ha sido ajeno a esta evolución en la legislación relacionada con la tecnología, como ejemplo esta el 2008, año en que se promulga la Ley 1245 que promueve y regula el Teletrabajo[69]; aunque como pasa con el Habeas Data o la Ley de Protección de Datos Personales, el Teletrabajo apenas está teniendo acogida, no solo entre los ciudadanos, también entre las empresas que evolucionan hacia este nuevo modelo y no tienen miedo a no tener a sus empleados al frente, a controlarles un horario de trabajo y a confiar en el logro de objetivos y en la autogestión.

Como en casi todo lo que tiene que ver con política y leyes, la legislación tecnológica no ha estado exenta de polémica y en los últimos tiempos esta palabra esta de la mano con Lleras, es decir, la Ley Lleras (en cualquiera de sus versiones teniendo en cuenta que algunos medios ya hablan de su "cuarta" versión a finales del 2013). Esta ley ha nacido como fruto de los compromisos adquiridos por Colombia con Estados Unidos y la Unión Europea de cara a los Tratados de Libre Comercio (esta ley es el perfecto ejemplo al segundo problema de la legislación en tecnología mencionado anteriormente) y está relacionada directamente con los derechos de autor y basada en la llamada Ley HADOPI[70], siendo incluso igual de polémica que su "equivalente" europea (considerando claro que la propuesta colombiana es menos agresiva o moderada). El objetivo de la llamada Ley Lleras (Proyecto de Ley 241 de 2011[71]) consiste en regular la responsabilidad de los ISP o proveedores de servicios de Internet frente a las infracciones de derechos de autor por parte de los usuarios, esto llevaba a la aplicación de penas

[69] CONGRESO DE LA REPÚBLICA. (06 de 10 de 2008). *Ley 1245 por la cual se establecen normas para promover y regular el teletrabajo y se dictan otras disposiciones*. Obtenido de Informática Jurídica: http://www.informatica-juridica.com/anexos/Ley_1221_de_16_de_julio_de_2008.asp

[70] HADOPI. (s.f.). *Haute Autoritépour la diffusion des ceuvres et la protection des droits sur internet*. Obtenido de HADOPI: http://www.hadopi.fr/en/haute-autorite/about-hadopi

[71] CONGRESO DE LA REPÚBLICA. (04 de 04 de 2011). *Proyecto de Ley 241 por el cual se regula la responsabilidad por las infracciones de derecho de autor y los derechos conexos en internet*. Obtenido de CONGRESO DE LA REPÚBLICA: http://servoaspr.imprenta.gov.co/gacetap/gaceta.mostrar_documento?p_tipo=05&p_numero=241&p_consec=28543

bastante severas, además de restricciones por parte de los ISP ante sospecha de violación de derechos (los servicios se reestablecían una vez el usuario demostraba que no infringía ley alguna) lo cual se entendía como la acción de un demandante sobre un usuario o sitio web (el bloque de un servicio) antes de realizar un debido proceso (se actuaba ante la sospecha, no después de confirmar la infracción).

El panorama actual de la legislación tecnológica en Colombia viene antecedido de un ya largo camino en el que cual se han introducido normas, se han modificado otras y simplemente se han eliminado algunas que ya no eran aplicables. No obstante es de considerar la falta de madurez que sobre este tipo de regulaciones existe en el país lo cual lleva a proyectos de ley que poco aportan al desarrollo tecnológico del país, lo anterior como resultado de la falta de preparación de muchos de los Senadores (muchos de ellos poco acercamiento tienen con la tecnología) además de las influencias externas y los intereses que se involucran en el desarrollo de estos proyectos, y en muchos casos de la poca participación que se deja a los profesionales en el área de la informática en el desarrollo de este tipo de normatividad.

4.4.2 Relación de delitos y leyes colombianas sobre seguridad informática y seguridad de la información.

Cuadro 1. Cuadro de delitos y leyes colombianas

Delito	Descripción	Leyes Aplicables	Sistema de Control
Distribución y\o Adquisición de software de forma ilegal	El delito relacionado con el software ilegal puede aplicar en dos sentidos: el primero es que el producto software de una empresa sea distribuido por terceros de forma ilegal, o que la organización adquiera e instale software no licenciado.	Ley 23 de 1982: Ley sobre derechos de autor**.** *Los autores de obras literarias, científicas y artísticas gozarán de protección para sus obras en la forma prescrita por la presente ley y, en cuanto fuere compatible con ella, por el derecho común.*	• Políticas de adquisición de software. • Políticas de instalación de software. • Políticas de control de acceso a internet y descarga de archivos. • Control en el licenciamiento de software.
Acceso no autorizado a comunicaciones de la organización	Consiste en la ejecución de acciones por medio de la cual se infiltran las comunicaciones telefónicas o las comunicaciones vía correo electrónico o chat y se obtiene información	Art. 192. Código Penal Violación ilícita de comunicaciones*: "El que ilícitamente sustraiga, oculte, extravié, destruya, intercepte, controle, o impida una*	• Encriptación de comunicaciones y mensajes. • Protocolo de comunicaciones. • Aseguramiento de equipos de

Delito	Descripción	Leyes Aplicables	Sistema de Control
	confidencial de una organización de forma ilegal.	*comunicación privada dirigida a otra persona, o se entere indebidamente de su contenido, incurrirá en prisión de uno a tres años, siempre que la conducta no constituya delito sancionado con pena mayor".*	comunicaciones mediante la implementación de VPN, Túnel IPSEC, entre otros. • Clasificación de la información y comunicaciones (nivel de privacidad, nivel de acceso).
Promocionar, vender y ofrecer software o hardware para ataques informáticos	Es común encontrar en la red sitios web que ofrecen aplicaciones e incluso dispositivos para llevar a cabo ataques informáticos, incluidos robos en cajeros automáticos.	Art. 192. Código Penal: Ofrecimiento, venta o compra de un instrumento apto para interceptar la comunicación privada entre personas. *El que, sin permiso de autoridad competente, ofrezca, venda o compre instrumentos aptos para interceptar la comunicación privada entre personas, incurrirá en multa siempre que la conducta no constituya delito sancionado con pena mayor.* Art. 269 E. Uso de software malicioso. *El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos*	• Control de acceso a internet. • Políticas de adquisición de software. • Políticas de instalación de software. • Control de los procesos internos de la organización.

Delito	Descripción	Leyes Aplicables	Sistema de Control
		legales mensuales vigentes.	
Ataque mediante inundación de PING	Está relacionado con la denegación de servicios, consiste en saturar un servidor u ordenador mediante solicitudes de respuesta PING hasta que el sistema no esté en capacidad de responder otras solicitudes y finalmente deje de responder.	Ley 1273 de 2009: *por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.* Art. 269 B. Obstaculización ilegítima de sistema informático o red de telecomunicación. *El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.*	• Aseguramiento de los equipos de comunicaciones. • Instalación de equipos de seguridad perimetral. • Políticas de acceso a la red. • Políticas de nombramiento de servidores (Evitar usar nombres evidentes como DBServer para nombrar servidores). • Bloqueo de acceso externos a servicios sensibles como PING, TraceRoute, Telnet, entre otros.
Ataque mediante fuerza bruta	Mediante ataques de fuerza bruta, generalmente intentando acceder a un sistema mediante la combinación de usuarios y contraseñas en base, por ejemplo, a	Art. 195. Código Penal: Acceso abusivo a un sistema informático. *El que abusivamente se introduzca en un sistema informático*	• Política de creación de usuarios y contraseñas. • Política de administración de contraseñas

Delito	Descripción	Leyes Aplicables	Sistema de Control
	diccionarios, se obtiene acceso a un sistema para ejecutar ataques mayores.	*protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo incurrirá en multa.* Art. 269 A. Acceso abusivo a un sistema informático: *El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.*	(tiempo de vigencia de contraseñas, numero de intentos de acceso con contraseña errónea para bloqueo de cuenta, etcétera). • Política de cancelación de cuentas. • Políticas de acceso externo a recursos en la red.
Ingeniería Social: Recolección de información	Se realiza envío de correos suplantando entidades legitimas para poder obtener información de forma "voluntaria" la cual posteriormente será vendida o usada para realizar ataques más fuertes.	Artículo 269 G. Suplantación de sitios web para capturar datos personales. *El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la*	• Capacitación continua del personal de la organización. • Políticas de control de acceso a internet. • Políticas de acceso y uso al correo corporativo. • Administración y gestión del sistema de correo electrónico de la organización.

Delito	Descripción	Leyes Aplicables	Sistema de Control
		conducta no constituya delito sancionado con pena más grave.	

Fuente: Propia

4.4.3 Ley de habeas data. El uso de la información de los ciudadanos por parte de las empresas, especialmente las privadas, había caído en vicios que fomentaban el uso no solo no regulado sino abusivo de los datos de los usuarios, siendo objeto de intercambios, campañas de publicidad molestas, y cualquier otra cantidad de situaciones en perjuicio de las personas. Sin embargo, en el año 2008 el Gobierno Nacional publicó la Ley Estatutaria 1266 en la cual se define lo relacionado con el Habeas Data y el manejo de bases de datos con información personal, y que a su vez reúne toda una serie de normas relacionadas con el tema pero que actuaban de manera separada (por ejemplo, el artículo 15 de la Constitución Política Colombiana, la Ley 1266 de 2008 y los fallos emitidos por la Honorable Corte Constitucional al respecto.

La Ley de Habeas Data busca proteger los datos del consumidor (básicamente del ciudadano en general) con el fin de que mantengan su carácter privado y que cada persona pueda hacer valer sus derechos frente a las entidades que hagan uso de ellos, puedan evitar del mal uso sus datos y de la venta a entidades que no están autorizadas, en pocas palabras, se trata de devolver el control al usuario sobre su información personal. En resumen, se puede definir la Ley de Habeas Data como el derecho fundamental del usuario para solicitar conocer la información que una empresa tiene sobre él, pero más importante aún puede solicitar que dicha información sea actualizada, rectificada o incluso retirada. Es una ley que aplica de obligatorio cumplimiento para todos los administradores de bancos de datos de cualquier naturaleza, incluyendo lo correspondiente a bases de datos de clientes, proveedores, contactos, etcétera[72].

- Últimos cambios sobre la ley de habeas data: Después de la publicación de la Ley 1266 en el año 2008 el gobierno ha realizado cambios y propuestas de modificaciones en pro de mejorar algunos aspectos de esta:
    - Proyecto de Ley 090/2014: Se proponen las siguientes modificaciones:

72 Es importante aclarar que los datos financieros están regulados bajo la ley 1266 de 2008 por lo que no están bajo la Ley de Habeas Data actual.

- Modificar los tiempos máximos de oportunidad de reporte negativo luego de entrar en mora.

- Oportunidad de notificación antes de efectuar un reporte negativo.

- Tiempo de permanencia del reporte negativo en las centrales de riesgo.

- Eliminación del reporte negativo en las Centrales de Riesgo.

- Estado de la calificación de una persona encontrándose en mora, al retirársele el reporte negativo y al ser consultada su información crediticia.

- Establecer beneficios a los ciudadanos por pago de su deuda en un determinado periodo de tiempo.

- Derechos de los usuarios: La Ley de Habeas Data otorga a los usuarios los siguientes derechos:

    - Los usuarios pueden hacer uso de los procedimientos de consultas o reclamos con el fin de ejercer el derecho fundamental al hábeas data.

    - Solicitar prueba que el titular de la información (es decir la persona natural o jurídica a la que hace referencia los datos que tiene la empresa) ha autorizado a la entidad para el uso de sus datos.

    - Solicitar información sobre las entidades y usuarios que tiene acceso a los datos del titular o usuario.

    - Solicitar el respeto sobre cualquier derecho constitucional o legal en el cual estén involucrados los datos personales de un usuario.

    - Acceder de forma gratuita a sus datos personales que hayan sido tratados por una entidad.

- Obligaciones de las entidades: Las entidades que posean datos personales están en obligación de:

    - Garantizar el buen uso de la información de los usuarios.

    - Rectificar la información de los usuarios cuando se considere necesario.

- Solicitar y conservar la autorización que da el usuario a la entidad para el uso y manejo de sus datos personales.

- Certificar semestralmente a las entidades de control que cuenta con la autorización del usuario para el manejo de la información.

- Informar al titular de los datos el tratamiento que se hará de los datos.

- Garantizar la seguridad necesaria para los datos personales y evitar la pérdida, adulteración o acceso no autorizado a los mismos.

- Garantizar que la información sea veraz, completa, exacta, actualizada, comprobable y comprensible.

- Rectificar la información.

- Dar gestión a las consultas, trámites y/o solicitudes que los titulares realicen en relación con sus datos personales.

- Definiciones relacionadas con la ley de habeas data: En relación con la ley de Habeas Data es importante considerar los siguientes términos:

    - En relación con el tratamiento de datos se considera que es cualquier acción relacionada con datos personales, desde su recolección hasta su eliminación de las bases de datos, incluido claro está, el uso de estos.

    - El organismo que realiza el tratamiento de datos requiere de la autorización o consentimiento expreso del titular de los datos para llevar a cabo cualquier acción sobre los mismos.

    - En cuanto al titular se hace referencia a la persona natural a la cual pertenezcan los datos que sobre los que se va a realizar algún tratamiento.

    - Los datos personales se refieren a cualquier información asociada o que pueda asociarse a una persona natural determinada.

    - Una base de datos es el conjunto de datos personales que son objeto de tratamiento.

    - Existe además un encargado del tratamiento, pero también un responsable del tratamiento. El primero es la persona o entidad que realice el tratamiento de datos personales, mientras que el segundo es la persona o entidad que decide sobre la base de datos o el tratamiento de los datos.

- Aplicabilidad de la ley: La ley de Habeas Data tiene la siguiente aplicabilidad:

    - Aplica a todos los datos personales registrados en cualquier base de datos sobre los que se pueda hacer tratamiento por alguna entidad.

    - Aplica a las entidades que efectúan tratamiento de datos en territorio colombiano o cuando la empresa aun encontrándose fuera del territorio nacional le sea aplicable legislación colombiano (incluidas las MiPyME en caso de contar con bases de datos de datos personales).

  Por otro lado, se puede mencionar que la Ley de Habeas Data no es aplicable en los siguientes casos:

    - Bases de datos de ámbito exclusivamente personal o doméstico.

    - Bases de datos cuya finalidad está relacionado con la seguridad nacional, defensa nacional, control de lavado de activos y financiamiento del terrorismo, o contenga información de inteligencia y contrainteligencia.

    - Bases de datos de información periodística y contenidos editoriales.

    - Bases de datos y archivos regulados por la Ley 1266 de 2008, así como las reguladas por la Ley 79 de 1993 correspondientes al Censo de Población y Vivienda.

4.4.4 Ley de delitos informáticos. Los delitos informáticos en Colombia son considerados penalmente dentro de la ley 1273 de 2009 y se incluyen los siguientes[73]:

- Acceso abusivo a un sistema informático: se relaciona con el acceso no autorizado a un sistema informático.

- La interceptación de datos informáticos: cualquier tipo de interceptación de datos sin el consentimiento de(los) propietario(s).

---

[73] CONGRESO DE LA REPÚBLICA. (05 de 01 de 2009). *Ley 1273 de 2009 por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado - denominado de la protección de la información y de los datos* . Obtenido de CONGRESO DE LA REPÚBLICA: http://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

- El uso de software malicioso: este apartado abarca todo lo relacionado con distribución y/o uso de software considerado como malicioso o dañino.

- Suplantación de sitios web: también conocido como *Phishing* es quizás una de las modalidades de delito informático más comunes (relacionados con la ingeniería social) y se encuentra contemplada en esta ley.

Las penas para los delitos incluidos en esta ley van desde los 48 meses hasta los 120 meses de prisión junto con multas según el delito cometido.

5 DISEÑO METODOLÓGICO

El proceso de diseñar un SGSI para la empresa Telemarketing S.A.S implica un conjunto de actividades a realizar para obtener una situación actual real de la organización y desde allí generar las acciones necesarias que permitan, al final del proyecto, completar el diseño.

Debido a las limitaciones geográficas asociadas al proyecto, el proceso de análisis y recopilación de información se llevará a cabo con el apoyo directo del Departamento de TI de la empresa Telemarketing S.A.S, partiendo desde el responsable de TI de la organización y sumando el equipo de Soporte, quienes a su vez realizarán el traslado de consultas y encuestas hacía las otras áreas que se involucren en alguna parte del proceso (Operación, Gestión Humana, Dirección). Dada esta situación el proceso la investigación analítica y descriptiva se realizará mediante encuestas y entrevistas dirigidas al Departamento de TI (descartándose la observación directa en sitio).

El proceso considera adicionalmente la revisión de la documentación con la que actualmente cuenta la organización, especialmente en lo referente a procesos, registros, manuales, entre otros y se trabajará en la generación de otros documentos como el inventario de activos y análisis de riesgos por medio del cual se pretende completar una imagen de la organización frente a la seguridad de la información.

5.1 METODOLOGÍA DE INVESTIGACIÓN

La investigación parte de la revisión sobre la situación actual de la empresa y la forma como está llevando a cabo sus procesos en la actualidad y como los ha documentado (si lo ha hecho), comparando con la norma y documentación relacionada. El proceso de investigación aplica la siguiente metodología:

Cuadro 2. Metodología de Investigación

Actividad	Objetivo	Metodología	Herramienta
Recolección de información	Información Primaria	1. Investigación y consulta con el personal de TI 2. Análisis de documentación y registros	1. Encuestas 2. Entrevistas 3. Documentación 4. Registros

Actividad	Objetivo	Metodología	Herramienta
	Información Secundaría	1. Bibliografía 2. Documentación General	1. Documentación
Inventario de activos	Valorar y relacionar los activos con el SGSI	1. Recolección de información por parte del Departamento de TI. 2. Tabulación de información 3. Valoración de activos	1. Inventario de activos 2. Formatos de Valoración de activos
Análisis e identificación de riesgos	Obtener la matriz de riesgos de la organización	1. Administración de riesgos en base a ISO\IEC 27005 2. Generación de matriz de riesgos. 3. Análisis y evaluación de riesgos.	1. ISO 27005 2. Matriz de Riesgos 3. Magerit

Fuente: Propia

5.2 METODOLOGÍA DE DESARROLLO

El proceso de desarrollo se basa en PHVA trabajado con base en el análisis previo:

- Planear (Diagnóstico de la situación actual): El diagnóstico de la situación actual está relacionado con la revisión de cómo la empresa está llevando a cabos sus procesos en la actualidad y como los ha documentado (si lo ha hecho), comparando con la norma y documentación relacionada.

Cuadro 3. Planear

Actividad	Objetivo	Metodología	Herramienta
Recolección de información	Información Primaria	1. Investigación y consulta con el personal de TI 2. Análisis de documentación y registros 3. Encuesta al Departamento de TI	1. Encuestas 2. Entrevistas 3. Documentación 4. Registros
	Información Secundaría	1. Bibliografía 2. Documentación General	1. Documentación
Inventario de activos	Valorar y relacionar los activos con el SGSI	1. Recolección de información por parte del Departamento de TI 2. Tabulación de información 3. Valoración de activos	1. Inventario de activos 2. Formatos de Valoración de activos

Actividad	Objetivo	Metodología	Herramienta
Análisis e identificación de riesgos	Obtener la matriz de riesgos de la organización	1. Administración de riesgos en base a ISO\IEC 27005 2. Generación de matriz de riesgos. 3. Análisis y evaluación de riesgos	1. ISO 27005 2. Matriz de Riesgos 3. Magerit

Fuente: Propia

- Planear – Hacer (Diseño del SGSI): El análisis previo permite tener una visión de la situación actual de la empresa en cuanto a seguridad de la información, y este a su vez se convierte en el insumo principal del diseño del SGSI de acuerdo con la norma ISO\IEC 27001:2013

Cuadro 4**.** Diseño del SGSI

Actividad	Objetivo	Metodología	Herramienta
Definición de políticas	Definir las políticas de acuerdo con el análisis realizado	1. Selección de políticas de acuerdo con ISO\IEC 27001:2013 2. Acuerdo con el área de TI de la organización 3. Acuerdo y compromiso con la Dirección	1. ISO\IEC 27001:2013 2. Matriz de riesgos
Seleccionar opciones de tratamiento de riesgos	Para el análisis de riesgos determinar las opciones para su respectivo tratamiento	1. Selección de opciones de tratamiento de riesgo 2. Acuerdo con el área de TI de la organización 3. Acuerdo y compromiso con la Dirección	1. ISO\IEC 27005 2. Matriz de riesgos
Seleccionar objetivos de control	Determinar los objetivos de control acordes con el análisis previo	1. Selección de controles Anexo A ISO 27001:2013. 2. Acuerdo con el área de TI de la organización.	1. ISO\IEC 27001:2013 ANEXO A
Definir Plan de Contingencia y Recuperación	Preparar los procedimientos para la recuperación operativa	1. Definición del plan de contingencia 2. Definición del plan de recuperación de desastres 3. Acuerdo con el área de TI de la organización	1. Plan de recuperación de desastres 2. Plan de Contingencia

Actividad	Objetivo	Metodología	Herramienta
Selección de criterios de evaluación	Medir mediante indicadores el comportamiento y evaluación del SGSI	1. Definir indicadores del SGSI 2. Acuerdo con el área de TI de la organización 3. Acuerdo con la Dirección de la organización	1. ISO\IEC 27001
Definición de acciones correctivas y preventivas	Determinar, en base al análisis realizado, las acciones correctivas y preventivas que permitan el cumplimiento del SGSI	1. Determinar acciones correctivas y preventivas 2. Seleccionar con el Departamento de IT la forma en que se realizaran las acciones correctivas y preventivas	1. ISO\IEC 27001

Fuente: Propia

- Hacer – Actuar (Implementación): El proceso de SGSI requiere de tener plasmado las fases anteriores en algo tangible y evaluable, es decir, procesos documentados, registro de las actividades, indicadores, entre otros. Esta fase no está incluida como parte del alcance del proyecto, pero se incluye como referencia para la organización.

Cuadro 5. Implementación

Actividad	Objetivo	Metodología	Herramienta
Redacción de los documentos base de la norma ISO\IEC 27001:2013	Desarrollar todos los documentos requeridos por la norma ISO\27001:2013	1. Desarrollar los documentos requeridos por la norma ISO 27001:2013 2. Uso de formatos establecidos o basados en normas de calidad 3. Definir control y versionamiento de los documentos	1. Formatos de documentación de procesos y procedimientos. 2. ISO\IEC 27001 3. ISO\IEC 9001
Documentación de los procesos y procedimientos	Documentar y disponer de los procesos y procedimientos	1. Documentar los procesos y procedimientos 2. Uso de formatos establecidos o basados en normas de calidad 3. Llevar control y versionamiento de los documentos	1. Formatos de documentación de procesos y procedimientos. 2. ISO\IEC 27001 3. ISO\IEC 9001

Actividad	Objetivo	Metodología	Herramienta
Registro de actividades y eventos	Disponer de un registro que permita medir el cumplimiento y avance de las políticas y controles	1. Desarrollar los registros documentales correspondientes a las políticas y controles 2. Uso de formatos establecidos o basados en normas de calidad 3. Llevar control y versionamiento de los documentos	1. Formatos de registros 2. ISO\IEC 27001 3. ISO\IEC 9001
Documentar plan de contingencia	Documentar el plan de contingencia de la organización	1. Desarrollar el plan de contingencia de la organización 2. Aprobar el plan de contingencia por parte de la Dirección 3. Compartir y capacitar las áreas involucradas en el plan de contingencia	1. Formatos de documentación de procesos y procedimientos 2. ISO\IEC 27001 3. ISO\IEC 9001
Documentar plan de recuperación de desastres	Documentar el plan de recuperación de desastres de la organización	1. Desarrollar el plan de recuperación de desastres de la organización 2. Aprobar el plan de recuperación de desastres por parte de la Dirección 3. Compartir y capacitar las áreas involucradas en el plan de recuperación de desastres	1. Formatos de documentación de procesos y procedimientos 2. ISO\IEC 27001 3. ISO\IEC 9001
Documentar procesos de evaluación del sistema	Definir, documentar y registrar los indicadores de evaluación del SGSI	1. Definir y documentar los indicadores 2. Definir Registro de indicadores y resultados 3. Documentar procedimientos de evaluación	1. ISO\IEC 27001:2013 2. Formatos de documentación de procedimientos y\o registros 3. ISO\IEC 9000

Fuente: Propia

5.3 UNIVERSO Y MUESTRA

Se limita el Universo al Departamento de TI de la empresa Telemarketing S.A.S, junto con los responsables de las áreas (Gestión Humana, Departamento Financiero, Operación) y por la Dirección de la empresa. Es importante señalar que por la naturaleza de la organización (Contact Center) entre el 80% y 90% de la población total corresponde a la base operativa (Agentes, Coordinadores, Auditores de Calidad, Formación) perteneciendo a un grupo que no está contemplado dentro del alcance del proyecto.

Cuadro 6. Población

Población	Número de Personas
Director Centro	1
Responsable Gestión Humana	1
Responsable Financiera	1
Responsable Operación	1
Responsable TI	1
Equipo de Soporte	3
Total	8

Fuente: Propia

Respecto a la muestra, teniendo en cuenta el tamaño de la población, se define que corresponde al 100% de la misma.

6 ESTADO DE LA ORGANIZACIÓN EN SGSI

Como punto inicial del desarrollo de la investigación se inicia con un diagnóstico de la organización en relación con seguridad de la información, tomando como guía los controles propuestos es la norma ISO 27001:2013. Es importante considerar en esta fase dos elementos importantes:

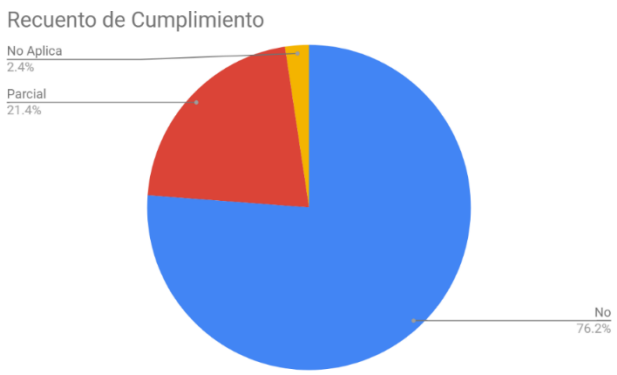
A) La organización no cuenta con un sistema implementado, ni ha estado antes expuesta a un proceso de auditoría de seguridad de la información o seguridad informática previo.

B) En esta fase se revisarán los controles y procesos que se considerarán para la implementación del SGSI enfocando los procesos principalmente al departamento de TI.

Aclarado lo anterior, se realiza el diagnóstico seleccionando los documentos que están relacionados con el SGSI (**ANEXO A. DIAGNÓSTICO INICIAL DOCUMENTACIÓN**), al igual que los procedimientos y controles que serán tenidos en cuenta en el proyecto (**ANEXO B. DIAGNÓSTICO INICIAL PROCESOS Y DOMINIOS**) considerando dos factores: a) Cumplimiento de cada punto y b) la documentación del procedimiento o control. Las respuestas de cada sección se encuentran registrados en los cuadros de los anexos 1 y 2, pudiendo destacar lo siguiente:

- Si bien la organización manifiesta cumplir con varios de los procedimientos y controles establecidos por la norma en sus anexos, en la práctica no existe documentación de una gran parte de ellos, bien sea explicando el proceso\control (procedimiento o manual) o registrando la ejecución de las actividades realizadas (formatos).

Figura 9. Cumplimiento de la documentación ISO 27001



Fuente: Propia

- Adicionalmente la organización en su intención de cumplir con los diferentes requerimientos de sus clientes, así como de diferentes organizaciones reguladoras, ha intentado implementar diferentes partes de la norma ISO 27001, sin una metodología, estructura e, igual que en el punto anterior, sin una documentación de los procesos. Por tal razón, lo avanzado hasta el momento en cuanto a la aplicación de la normal en la organización presenta los siguientes inconvenientes:

    - Si bien han desarrollado una serie de políticas de seguridad, estas no están organizadas, documentadas ni son revisadas bajo un procedimiento debidamente establecido.

    - Las políticas de SGSI no son parte de las actividades diarias de la organización.

    - No hay capacitación sobre la seguridad de la información en la organización, por lo que las políticas implementadas no son de conocimiento de los miembros de la organización de forma efectiva.

    - Se encuentran en estado crítico, bien sea por falencias en implementación o por falta de documentación, los siguientes aspectos de la norma:

        - Control de acceso.
        - Criptografía.
        - Operaciones.
        - Adquisición, gestión y mantenimiento de equipos.
        - Incidentes de seguridad.
        - Continuidad.

- Cumplimiento.

Se han desarrollado también dos encuestas, la primera enfocada directamente al área de IT, y la segunda más general para ser respondida por los empleados de la organización. Mediante estas encuestas se busca principalmente obtener unos indicadores de parte del personal de la empresa relacionados con la seguridad de la información.

A nivel de TI se realizaron las siguientes preguntas:

- Información General
    - ¿En qué sector de la economía se encuentra la organización?
    - ¿Cuántos empleados tiene la organización?
    - De la cantidad reportada anteriormente, ¿cuántos son empleados internos?
    - De la cantidad reportada anteriormente, ¿cuántos son externos u outsourcing?
    - ¿Cuenta la organización con un área de TI propia?
    - ¿Cuenta la organización con un área o grupo de seguridad de la información?
- De las siguientes herramientas\soluciones para seguridad de la información, ¿Cuáles son usadas por la organización actualmente?
    - Control de acceso mediante usuario y contraseña.
    - En caso afirmativo ¿qué herramienta usa?
    - ¿Cuenta con un sistema propio para encriptación de archivos y/o mensajes?
    - ¿Cuenta con sistema de respaldo de archivos?
    - ¿Cuentan con control de acceso a espacios de TI?
    - En caso afirmativo, ¿qué tipo de control usa?

- ¿Cuenta la empresa con software antivirus?
- ¿Usa la empresa software privado o comercial?
- ¿Usa la empresa software libre u open-source?
- ¿Conoce la empresa los tipos de licencia requeridos para software y hardware usado?
- ¿Cuenta la empresa con todas las licencias requeridas para el software y hardware usado?
- ¿Cuenta la empresa con sistemas de protección perimetral (Firewalls)?
- ¿Tiene la organización un plan de adquisición\mejora de sistemas de protección de seguridad de la información?

- Estadísticas sobre seguridad de la información
  - ¿Ha tenido la empresa incidentes relacionados con seguridad de la información en los últimos 12 meses?
  - En caso afirmativo ¿cuál es el promedio mensual de incidentes detectados?
  - De los incidentes detectados, ¿cuál es el porcentaje de los incidentes internos?
  - De los incidentes detectados, ¿cuál es el porcentaje de los incidentes externos?
  - En caso afirmativo a las anteriores preguntas, ¿cuál es el top 5 de origen de los incidentes?
  - En caso afirmativo a las anteriores preguntas, ¿cuál es el top 5 de los tipos de incidentes?

A nivel general se realizaron las siguientes preguntas (seguidas de las correspondientes respuestas):

- Información General
  - ¿En qué área de la organización laboral actualmente?

Es claro que el área crucial de la empresa es la operativa, considerando que los agentes o ejecutivos comerciales son la mayor proporción en cuanto a empleados y que son los que realizan las actividades núcleo del negocio. Es importante señalar que aún con los diferentes esfuerzos realizados no fue posible obtener más de un 10% de encuestados sobre la población total, esto refleja el poco compromiso general de la organización en temas relacionados con la seguridad de la información, un problema clave a resolver para el éxito del SGSI.

Figura 10. Áreas que responden la encuesta

Fuente: Propia

- ¿Cuánto tiempo lleva en la organización?

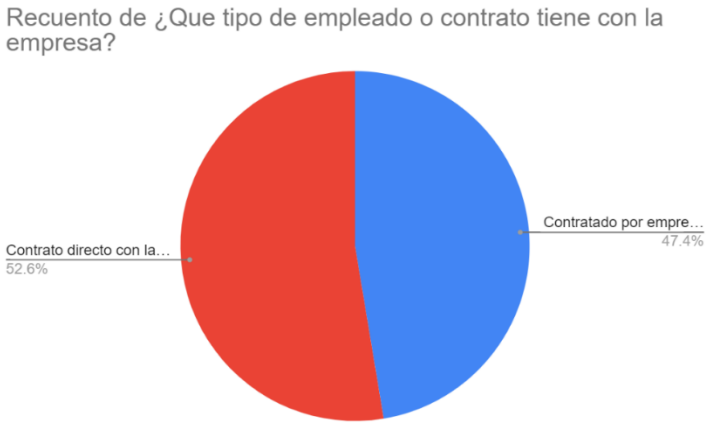
Figura 11. Tiempo de vinculación en la empresa

Fuente: Propia

Mas del 47% del personal encuestado tiene menos de un año dentro de la organización, esto se presenta debido a la alta rotación que presentan los centros de contacto, donde la retención de personal es complicada y los puestos que se mantienen durante largo tiempo suelen ser los cargos administrativos. Esto refleja un nuevo problema en la implementación del SGSI, puesto que una cantidad importante del personal que sea capacitado se retirará antes de cumplir el año y casi un 60% ya no hará parte de la empresa al segundo año, lo que implica que en un corto periodo de tiempo no se estará hablando de un refuerzo en las capacitaciones de SGSI, sino de un comienzo del proceso.

- ¿Es empleado(a) interno(a) o externo(a)\outsourcing?

Figura 12. Tipo de contrato



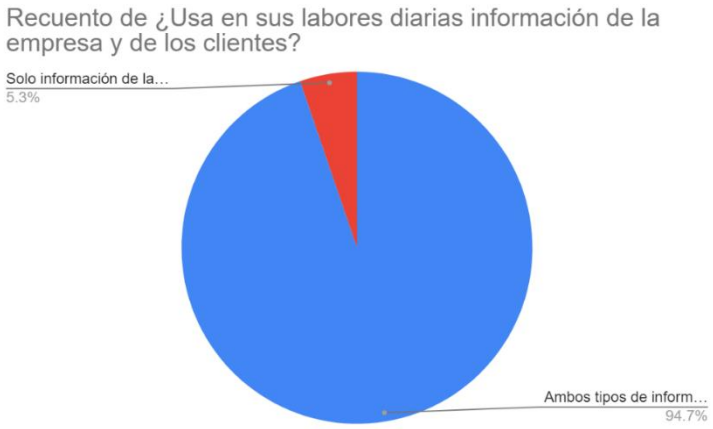
Fuente: Propia

Un alto porcentaje de las personas contratadas se vinculan mediante una empresa externa (subcontratación), esto influye a nivel de SGSI en las políticas de contratación, pues están sujetas también a la empresa mediante la cual se realiza la vinculación de poco más del 47% de los empleados.

- ¿Conoce usted el área de TI de la organización? Para esta pregunta el 100% de los encuestados indican conocer el área de TI.

- ¿Maneja en sus labores diarias información sensible de la organización?

Figura 13. Uso de la información



Fuente: Propia

Este punto es de suma importancia para el SGSI, pues refleja que el compromiso en la protección de la información no es un tema únicamente interno, sino también implica la información de los clientes (y a su vez los clientes de estas empresas que contratan con la organización), un compromiso importante no solo a nivel de imagen y prestigio de la empresa, sino también la influencia que tiene con los contratos y acuerdos comerciales.

- ¿Usa en sus labores diarias equipos tecnológicos (PC, laptop, tablet, teléfono móvil, etcétera)?

  En esta pregunta se identifica lo siguiente:

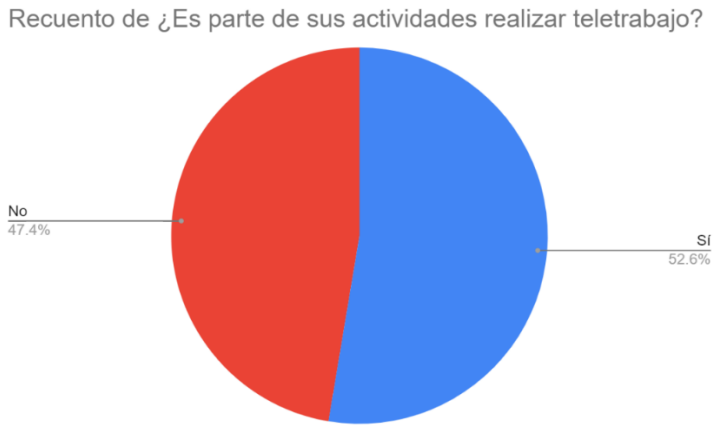
  - El 100% de los empleados hace uso de computador, bien sea este un ordenador de escritorio o laptop.

  - El 52% de los empleados hace uso de teléfono móvil para sus labores, lo cual es un dato que debe ser analizado puesto que no es habitual en los *Contact Center* los agentes usen dispositivos móviles.

  - El 5.3% de los empleados informan que hacen uso de memorias extraíbles en sus funciones, impresora y escáner.

- ¿Es parte de sus actividades realizar teletrabajo?

Figura 14. Teletrabajo en la organización



Fuente: Propia

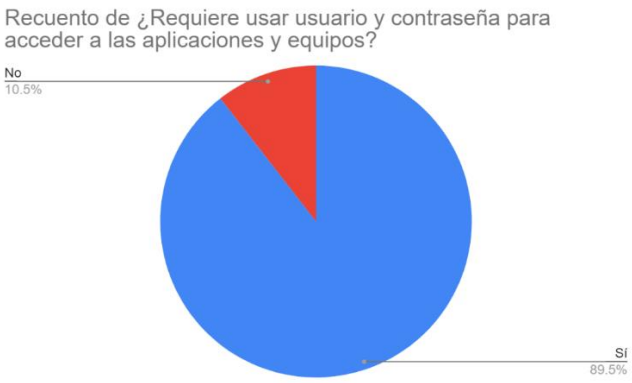
El teletrabajo es parte considerable de las operaciones de la organización, por lo que es un punto para tener en cuenta en la implementación del SGSI.

- De las siguientes herramientas relacionadas con la información y la tecnología, ¿cuáles usa en sus labores?

    - Acceso y contraseña para el acceso a todas las aplicaciones y equipos.

      Si bien una gran mayoría informan el uso de credenciales de acceso a los recursos informáticos de la empresa, existe un porcentaje mayor al 10% que no lo hacen. Es un punto que debe ser asegurado al 100% para mejorar la seguridad de la información en la organización.

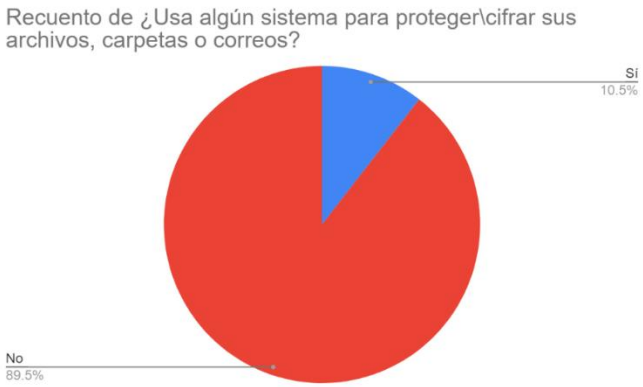
Figura 15. Credenciales de acceso a los sistemas



Fuente: Propia

- Usa sistema de cifrado\protección de archivos, carpetas y correos.

Figura 16. Uso de cifrado

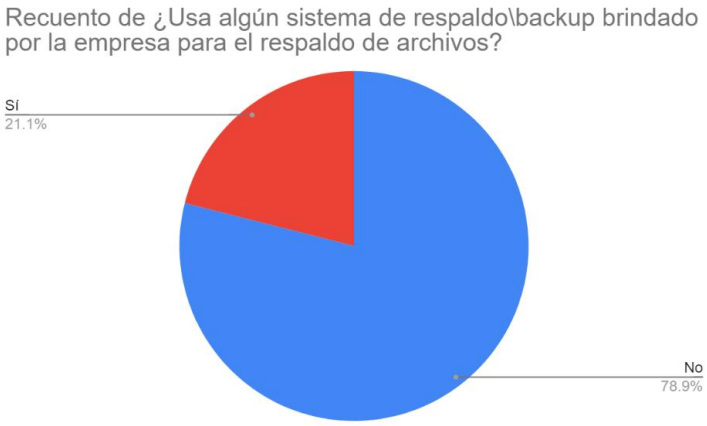


Fuente: Propia

A pesar de manejar información propia y además de los clientes, el uso de mecanismos de cifrado es mínimo, lo cual va en detrimento de la seguridad de la información.

- ¿Usa el sistema de respaldo\backup de archivos? En caso negativo, ¿por qué no lo usa?

Figura 17. Uso de backup de archivos

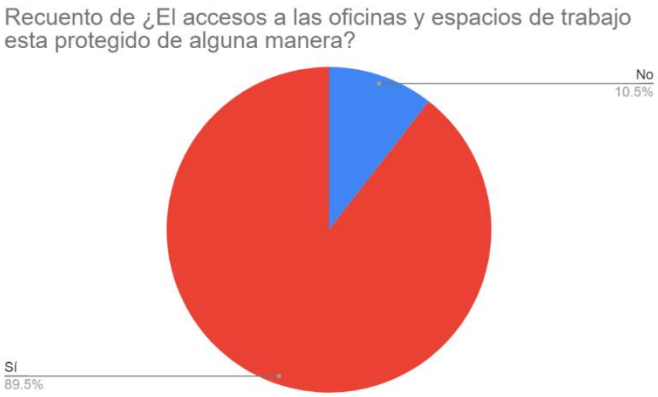


Fuente: Propia

Otro punto delicado detectado en la encuesta muestra que poco más del 20% hace uso de sistemas de respaldo de la información, lo cual permite evidenciar la falta de protección de los datos dentro de la organización. Entre las respuestas se señala que el sistema de backup para usuarios dejó de estar operativo, razón por la cual muchos usuarios no hacen copias de seguridad de sus archivos, o en algunos casos respaldan la información en sistemas públicos y personales de respaldo, como One Drive, Mega, Google Docs, etcétera.

- ¿El acceso a las oficinas y espacios privados están protegidos de alguna manera?, ¿Qué mecanismos de protección conoce?

Figura 18. Acceso físico controlado



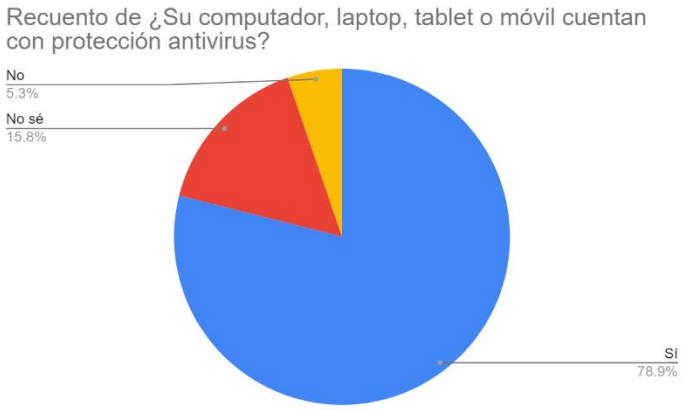
Fuente: Propia

El acceso físico a zonas de la empresa se encuentra protegido y controlado en su mayor parte.

- ¿Su computador\laptop\teléfono móvil cuenta con protección antivirus?

El software antivirus es fundamental en la protección de los equipos tecnológicos, si bien un gran porcentaje manifiesta tener sus dispositivos protegidos existe una proporción aun importante que no cuentan con este tipo de software, adicionalmente, es importante considerar el licenciamiento del software y las actualizaciones.

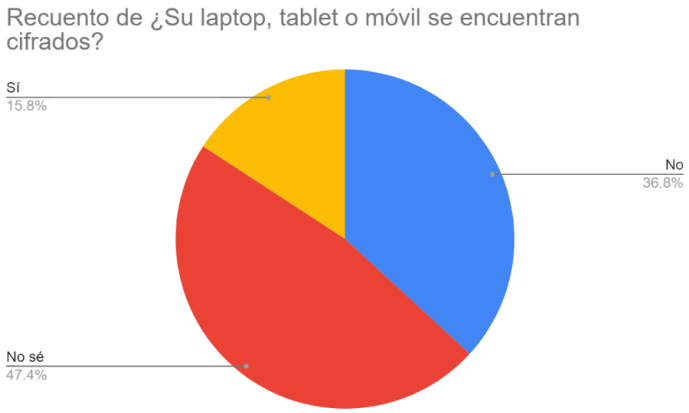
Figura 19. Uso de software antivirus



Fuente: Propia

- ¿Su laptop, Tablet o móvil se encuentran cifrados?

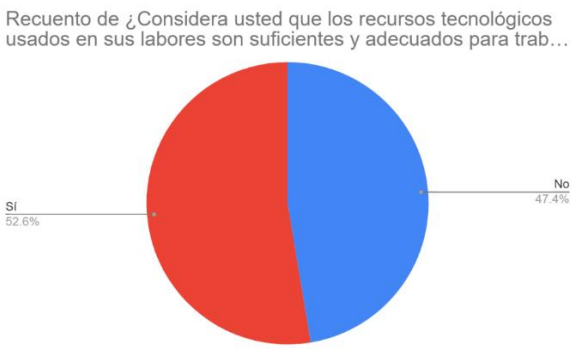
Figura 20. Cifrado de equipos



Fuente: Propia

- ¿Considera usted que los recursos tecnológicos usados en sus labores son suficientes y adecuados para trabajar?

Figura 21. Características de los equipos



Fuente: Propia

- En caso negativo en la respuesta a la pregunta anterior indique la razón.

  En complemento a la pregunta anterior se ha solicitado información sobre la razón por la que no se consideran óptimos los equipos asignados actualmente. Las razones expresadas corresponden a:

  - Problemas en cuanto a disponibilidad de equipos para reemplazar unidades defectuosas.
  - Equipos con características de hardware limitadas o sin el software necesario para realizar actividades.
  - Uso de equipos personales para funciones laborales debido a falta de recursos para asignar.

- ¿El uso de Internet es necesario para la ejecución de sus labores?

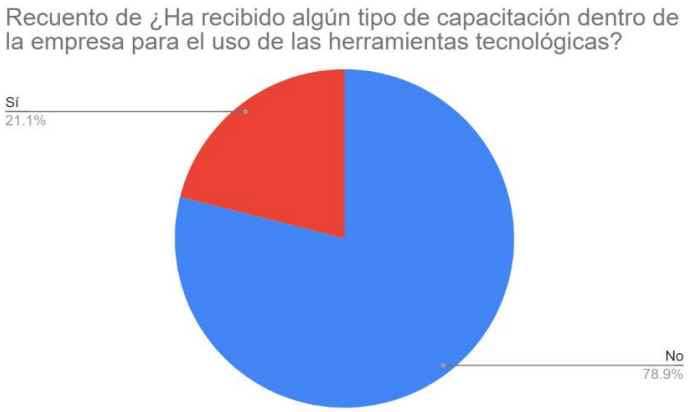
  El 100% manifiesta que el uso de internet es necesario para sus labores.

- ¿Ha recibido algún tipo de capacitación en el uso de herramientas tecnológicas (Colegio, universidad, cursos, etcétera)?

  En relación con la capacitación en el uso de recursos tecnológicos todos los encuestados manifiestan tener algún grado de capacitación, lo cual es importante para el uso de dichos recursos y para los procesos de capacitación en SGSI.

- ¿Ha recibido algún tipo de capacitación dentro de la empresa para el uso de las herramientas tecnológicas?

Figura 22. Capacitación interna sobre herramientas informáticas



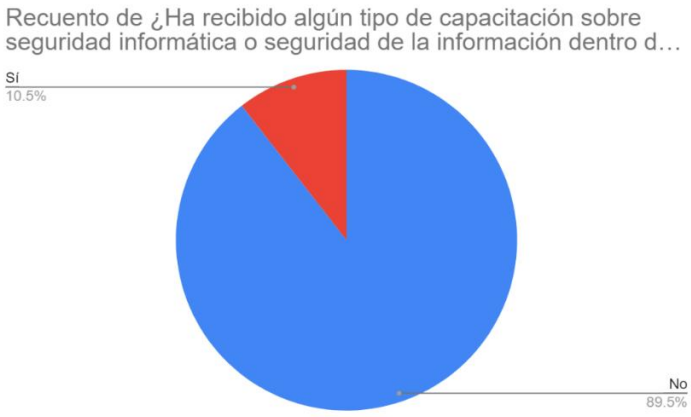
Fuente: Propia

En contraste con el punto anterior, la capacitación interna en herramientas tecnológicas es bastante baja (21.1%), una cifra preocupante en una organización en la cual un altísimo porcentaje de sus funciones se realizan en ordenadores y apoyados en diferentes herramientas de software.

- ¿Ha recibido algún tipo de capacitación sobre seguridad informática o seguridad de la información dentro de la empresa?

  Puede considerarse más crítico identificar que solo un poco más del 10% manifiestan recibir capacitación en seguridad informática o seguridad de la información.

Figura 23. Capacitación interna SGSI



Fuente: Propia

- Estadísticas sobre seguridad de la información

  - ¿Ha sufrido usted o alguno de sus compañeros algún incidente informático dentro de la organización?

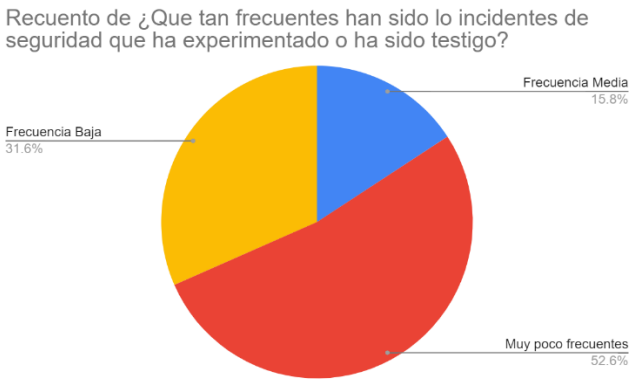
Figura 24. Incidentes de seguridad

Fuente: Propia

Este punto indica que una alta cantidad de personas que han percibido o sufrido un incidente de seguridad informático dentro de la organización. Es un porcentaje bastante alto, quizás compensado por la frecuencia con que se presentan dichos incidentes (ver el punto siguiente), pero igual de importancia para la organización.

  - ¿Qué tan frecuentes han sido los incidentes de seguridad que ha experimentado o ha sido testigo?

Figura 25. Frecuencia de incidentes



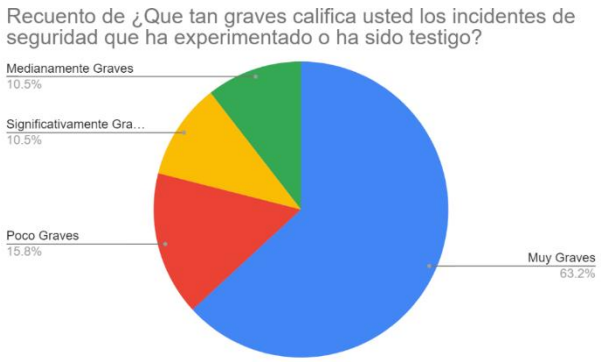
Fuente: Propia

El dato del punto anterior contrasta con la frecuencia de los incidentes, si bien un alto porcentaje indica sufrir de incidentes de seguridad, la frecuencia resulta ser muy baja o baja.

- ¿Qué tan graves califica usted los incidentes de seguridad que ha experimentado o ha sido testigo?

  Si bien el punto anterior indica que la frecuencia de los incidentes es baja, la gravedad de ellos es importante, casi un 85% están por encima de incidentes de mediana gravedad, es decir, aunque se presentan en poca frecuencia cuando se dan el efecto en la organización es significativo.

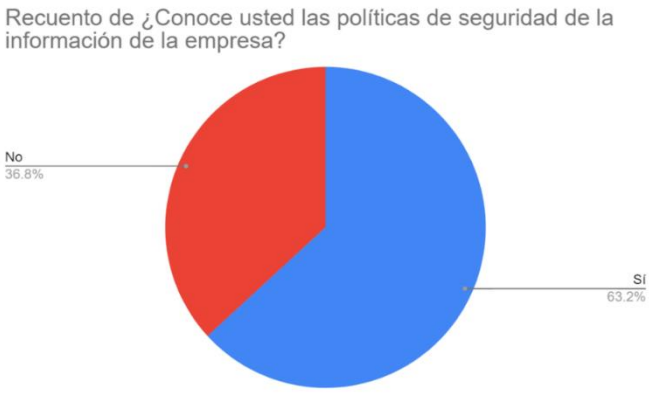
Figura 26. Gravedad de los incidentes



Fuente: Propia

- ¿Conoce usted las políticas de seguridad de la información de la empresa?

Figura 27. Conocimiento políticas de seguridad de la información



Fuente: Propia

Un importante porcentaje indica conocer las políticas de seguridad de la información. Aunque contrasta con la pregunta sobre las capacitaciones internas de la empresa, es un indicador del esfuerzo de la organización para implementar políticas de seguridad.

- ¿Identifica usted el área o la persona responsable de la seguridad de la información de la empresa?

Figura 28. Identificación del responsable de seguridad

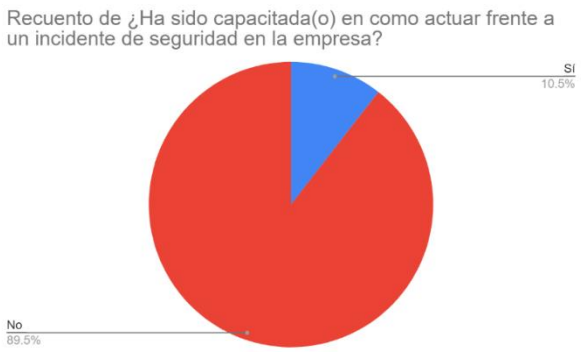
Fuente: Propia

Dentro de la organización se reconoce o identifica el papel del responsable de seguridad de la información. Esto es un paso positivo en el proceso de implementar un SGSI en la empresa.

- ¿Ha sido capacitada en cómo actuar frente a un incidente de seguridad en la empresa?

Este punto se puede identificar como una confirmación a la anterior pregunta sobre capacitación en seguridad de la información dentro de la empresa. Capacitación es quizás uno de los puntos más significativos a tratar en la implementación del SGSI.

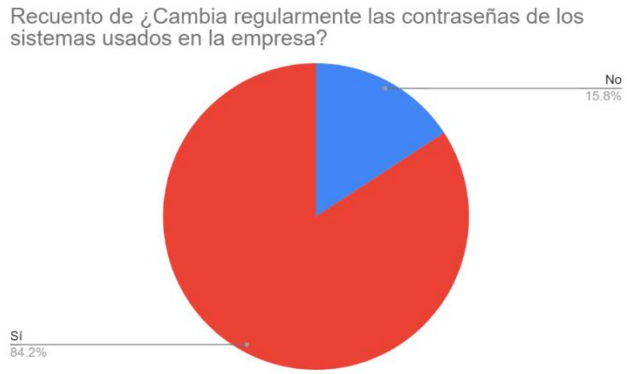
Figura 29. Capacitación frente a incidentes de seguridad



Fuente: Propia

- Buenas prácticas de seguridad de la información
    - ¿Cambia regularmente las contraseñas de los sistemas usados en la empresa?

Figura 30. Cambio de contraseñas

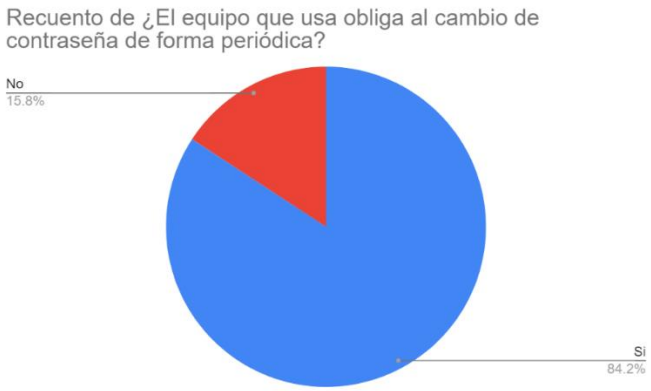


Fuente: Propia

En cuanto a buenas prácticas con la contraseña hay también avances respecto al cambio periódico de las mismas, sin embargo, la existencia de un 15% que no lo realiza puede significar que las medidas que obligan el cambio de clave no son efectivas o están bien establecidas.

- ¿El equipo que usa obliga al cambio de contraseña en forma periódica?

Figura 31. Cambio obligatorio de contraseña



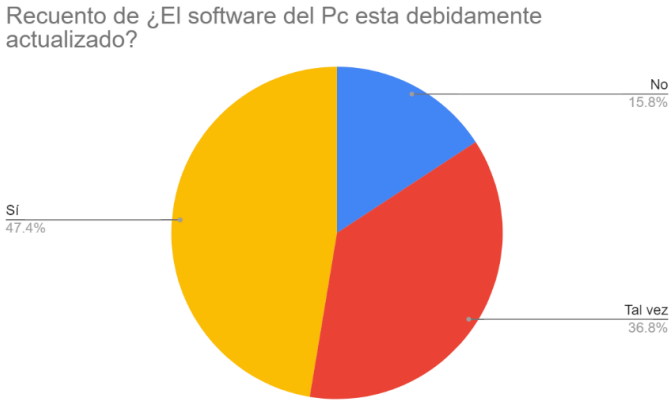
Fuente: Propia

Complementando el punto anterior, existe una mala aplicación de políticas de seguridad de las contraseñas o una serie de excepciones que deben ser analizadas y documentadas.

- ¿El software del Pc está debidamente actualizado?

Existe incertidumbre sobre el estado de las actualizaciones del PC, esto en parte por falta de capacitación al respecto, por pocas posibilidades de tener acceso a esta información, y finalmente a una ausencia de políticas de actualización que se cumplan correctamente.

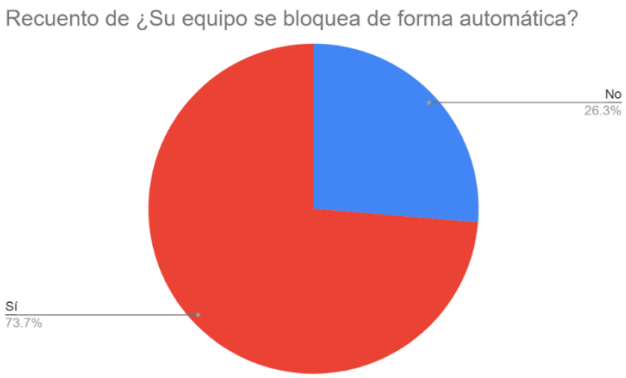
Figura 32. Actualización de equipos



Fuente: Propia

- ¿Su equipo se bloquea de forma automática?

Figura 33. Bloqueo de equipos

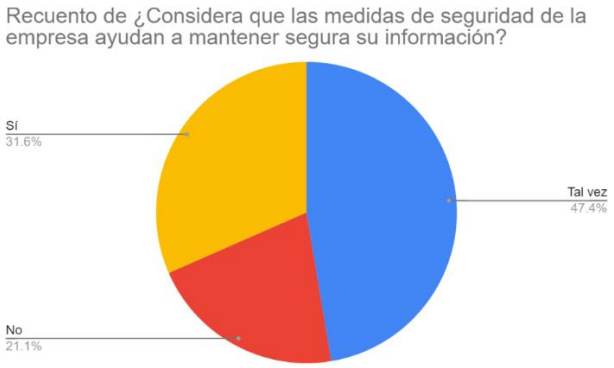


Fuente: Propia

Siguiendo con las buenas prácticas de seguridad se consulta a los usuarios algunas características que se suelen considerar como básicas, en este caso el bloqueo automático. Igual que en el caso del cambio de contraseñas se nota una aplicación de la política mayoritaria, pero no es aplicada al 100% de la organización, lo cual puede ser por excepciones no documentadas, o por error en la gestión de la política.

- ¿Considera que las medidas de seguridad de la empresa ayudan a mantener segura su información?

Figura 34. Percepción sobre las medidas de seguridad



Fuente: Propia

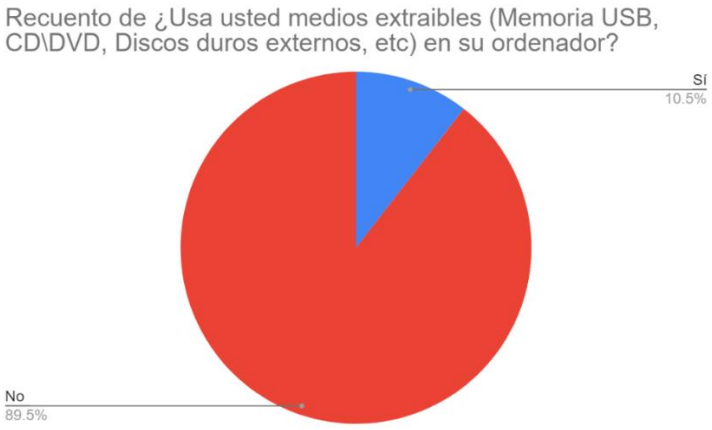
La percepción de los empleados sobre las medidas de seguridad que se emplean actualmente en la organización es ambigua, aproximadamente el 52% tienen una respuesta clara y concreta a favor o en contra de las medidas de seguridad, pero existe casi un 48% que no están seguros (aun cuando un alto porcentaje reporta que se han presentado incidentes).

En este sentido es importante dar confianza a los integrantes de la organización sobre los esfuerzos de la empresa para preservar la seguridad de la información, evitando dudas y haciéndolos parte del SGSI.

- ¿Usa usted medios extraíbles (Memoria USB, CD\DVD, Discos duros externos, etcétera) en su ordenador?

  Sobre las buenas prácticas se realiza esta pregunta para conocer el uso de dispositivos móviles dentro del a empresa, un factor de riesgo que debe ser correctamente controlado.

Figura 35. Uso de medios extraíbles



Fuente: Propia

- ¿Ha compartido las contraseñas con sus compañeros?

Figura 36. Cuidado de las contraseñas

Fuente: Propia

Una última pregunta sobre buenas prácticas está relacionada con el cuidado de las credenciales de acceso, en donde se evidencia una falta de capacitación aun del personal de la organización teniendo en cuenta el 21% que acepta haber compartido sus credenciales de acceso. Esto implica a) una buena capacitación del personal, b) medidas para evitar el préstamo de datos sensibles y credenciales de acceso, y c) aplicar medidas que impidan el uso de recursos tecnológicos con datos de acceso no permitidos.

6.1 FICHA TÉCNICA

Se presenta a continuación la ficha técnica de la encuesta:

- Objetivo: Conocer o realizar un sondeo sobre las condiciones de la organización en cuanto a buenas prácticas de seguridad de la información.
- Tipo de encuesta: descriptiva
- Metodología: Recolección de información a través de cuestionario específico.
- Técnica de recolección
  - Cuestionario Electrónico
- Ámbito
  - Ámbito poblacional: Empleados de la organización Telemarketing S.A.S
  - Ámbito geográfico: Esta encuesta ha sido realizada en la sede ubicada en Colombia.
  - Ámbito Temporal: Encuesta realizada una única vez.
- Tamaño de la muestra:

    - 19 empleados de la organización pertenecientes a las áreas de Tecnología (IT), Operaciones, Formación, Calidad, Recursos Humanos, Administrativa y Business Intelligence (BI)
- Fecha de recolección de la información:
    - 25/09/2019 al 04/10/2019
- Diseño y Realización
    - La encuesta fue realizada por Germán Andrés Olano Trejos, estudiante de la especialización en Seguridad Informática

7 INVENTARIO DE ACTIVOS

El análisis realizado con la organización ha permitido identificar los activos de información relacionados con el área de IT. El proceso de obtención de la información se apoyó directamente en el personal del departamento de TI de la organización y los activos se han agrupado para hacer fácil análisis (especialmente para herramientas de apoyo como PILAR).

La agrupación se ha centrado en relacionar los diferentes activos en uno solo más general. Tomando como ejemplo el servidor:

- Activo: Hardware (HW)
    - Grandes equipos (HOST).
- Activo: Software (SW)
    - Sistema Operativo Windows.
    - Sistema Operativo Linux.
    - Servidor de presentación.
    - Servidor de aplicaciones.
    - Servidor de directorio.
    - Servidor de ficheros.
    - Sistema de gestión de bases de datos.
- Activo: Datos de Información (D)
    - Datos de configuración.
    - Registros de actividad.
- Activo: Servicios (S)
    - Interno – Usuarios.
    - Almacenamiento de ficheros.
    - Servicio de impresión.
    - Transferencia de archivos.
    - Servicio de copias de respaldo.
    - Servicio de directorio.
    - Servidor de nombres de dominio.
    - Gestión de identidades.
    - Gestión de privilegios.

- Soportes de Información (Media)
    - Discos.
    - Almacenamiento en Red.

El listado de activos se presenta en el siguiente subcapítulo junto con su valoración.

7.1 VALORACIÓN DE LOS ACTIVOS EN LOS DOMINIOS

El proceso de valoración de activos en los dominios se ha planteado desde lo cualitativo, dimensionando el valor que tiene el activo para la operación y la continuidad del negocio. A su vez los dominios que se consideran son los siguientes:

[D] Disponibilidad: De qué manera o en qué nivel impacta en la operación que un activo no se encuentre disponible.

[I] Integridad: Cuál es el impacto generado por un activo que ha sido modificado sin autorización o control por parte de la organización.

[C] Confidencialidad: En qué medida afecta que un activo sea accesible por un usuario no autorizado o por alguien externo.

[A] Autenticidad: Importancia de identificar el usuario o entidad que accede al activo.

[T] Trazabilidad: Importancia de mantener un seguimiento (o traza) sobre el uso y\o acceso del activo.

Cuadro 7. Valoración de activos

Valor Asignado	Criterio Valoración
10	Muy alto valor para la operación, no hay continuidad del negocio, no se puede operar.
8-9	Alto valor para la operación, dificultades para operar sin el activo, afecta parte de la continuidad del negocio.
6-7	Valor normal para la operación, afecta la operación, pero no la continuidad del negocio.
3-5	Bajo valor para la operación, el efecto en la operación es bajo, no afecta continuidad del negocio.
1-2	Muy bajo valor para la operación, no se percibe efecto en la operación ni en la continuidad del negocio.

Fuente: Propia

El resultado de aplicar la valoración para cada activo en el dominio correspondiente es el siguiente:

Cuadro 8. Inventario de Activos y Valoración

Grupo	Nombre	D	I	C	A	T	Valor Acumulado	Valor Cualitativo
Activos Esenciales	Servicio Telefonía	10	9	7	9	8	10	Muy Alto
	Red LAN Operativa Voz y Datos	10	10	0	3	0	10	Muy Alto
	Servicio de gestión de marcación telefónica	10	10	9	9	7	10	Muy Alto
	Base de datos operativa	10	10	9	3	10	10	Muy Alto
Personal	Personal operativo	7	7	7	0	0	7	Normal
	Personal administrativo RRHH\Finanzas\Gerencia	7	7	7	0	0	7	Normal
	Personal estructura operativa	5	5	7	0	0	7	Normal
Instalaciones	Edificio General	9	9	7	0	3	9	Alto
	Centro de datos	10	9	10	0	7	10	Muy Alto
	Locaciones operativas y administrativas	9	5	8	0	3	9	Alto
Servicios Subcontratados	Servicios generales mantenimiento	4	0	0	0	0	4	Bajo

Grupo	Nombre	D	I	C	A	T	Valor Acumulado	Valor Cualitativo
	Servicio de página web	5	5	0	0	1	5	Bajo
	Servicio de correo electrónico	5	6	6	5	0	6	Normal
	Servicio de líneas móviles	4	3	3	0	0	4	Bajo
Equipamiento Aplicaciones	Software ofimático	4	3	0	7	0	7	Normal
	Software antivirus	7	3	0	0	3	7	Normal
	Software Administrativo-Contabilidad-RRHH	9	7	8	7	4	9	Alto
Equipamiento Equipos	Equipos de escritorio - laptops	9	5	7	0	0	9	Alto
	Servidores	10	9	9	10	7	10	Muy Alto
	Equipos de telefonía móvil	5	4	5	0	0	5	Bajo
Equipamiento Elementos Auxiliares	Sistema de alimentación ininterrumpido	10	0	0	0	5	10	Muy Alto
	Generador eléctrico de respaldo	9	0	0	0	5	9	Alto
	Cableado eléctrico Centro	9	0	0	0	0	9	Alto
	Cableado fibra óptica	9	0	0	0	5	9	Alto
	Impresoras	2	0	0	0	0	2	Muy Bajo
	Servicio *Backups*	9	9	9	9	5	9	Alto
Equipamiento Comunicaciones	*Switches Core* y Distribuidores	9	0	0	3	7	9	Alto
	Firewall	10	3	7	3	7	10	Muy Alto
	Canal de internet principal y *Backup*	7	7	3	3	3	7	Normal
	Canal de MPLS casa matriz Principal y *Backup*	7	7	7	7	7	7	Normal
	Cableado estructura voz y datos	9	7	7	7	7	9	Alto
Servicios Internos	Serv. Técnicos Auxiliares Ficheros configuración	5	3	5	0	0	5	Bajo
	Serv. Técnicos Auxiliares Manuales y Procedimientos	5	3	5	0	0	5	Bajo
	Servicio de servidor de archivos	7	7	7	7	3	7	Normal
	Servicio de base de datos administrativa	7	7	7	7	3	7	Normal

Fuente: Propia

8 ANÁLISIS DE RIESGOS

8.1 AMENAZAS

La identificación de amenazas se realiza considerando la documentación de MAGERIT y apoyado en las relaciones que automáticamente genera la herramienta Pilar para distintos tipos de activos. Se parte entonces de considerar para cada activo las amenazas que le pueden afectar y la forma en que lo hacen (en otras palabras, la degradación sobre el activo). Un ejemplo de esto es las instalaciones físicas las cuales pueden estar expuestas a los incendios, y en caso de que esta amenaza se materialice, puede suponer una degradación del 100% del activo, es decir la pérdida completa.

Posterior a obtener el impacto (Impacto = valor del activo * degradación), se debe considerar cuan frecuente o probable que la amenaza se materialice sobre un activo. Probablemente un incendio en las instalaciones físicas es algo que no suceda nunca (sería catastrófico para la empresa) por lo que tendría una ocurrencia extremadamente difícil, mientras que una situación como que los empleados usen los ordenadores para actividades diferentes a las que han sido destinadas es muy fácil, probablemente pasando a diario. Para definir la tabla de valoración se toma como apoyo los criterios de la herramienta PILAR y la documentación de MAGERIT, quedando de la siguiente forma:

Cuadro 9. Valoración de la probabilidad de ocurrencia

Valor	Criterio	Facilidad
100	Diario	Fácil
10	3 o 4 veces al mes	Medio
1	4 veces al año	Difícil
0,1	1 vez al año	Muy difícil
0,01	Casi ninguna	Extremadamente difícil

Fuente**:** Propia

La tabla 10 permite observar para cada activo las amenazas relacionadas y la degradación de dichas amenazas pueden causar en cada dimensión (esto es el **impacto**). Luego, aplicando la fórmula directa, se calcula el impacto en cada dimensión.

Cuadro 10. Selección y valoración de amenazas

Nombre	Amenaza	D	I	C	A	T	D	I	C	A	T
		Degradación					Impacto				
[B][S]Servicio Telefonía											
	[I.5]Avería de origen físico o lógico	50%					5,0	0,0	0,0	0,0	0,0
	[I.8]Fallo de servicios de comunicaciones	100%					10,0	0,0	0,0	0,0	0,0
	[E.2]Errores del administrador del sistema\de la seguridad	20%	20%	20%			2,0	1,8	1,4	0,0	0,0
	[E.8]Difusión de software Dañino	10%	10%	10%			1,0	0,9	0,7	0,0	0,0
	[E.9]Errores de [re-]encaminamiento			10%			0,0	0,0	0,7	0,0	0,0
	[E.10]Errores de secuencia		10%				0,0	0,9	0,0	0,0	0,0
	[E.15]Alteración de información		10%				0,0	0,9	0,0	0,0	0,0
	[E.18]Destrucción de la información	10%					1,0	0,0	0,0	0,0	0,0
	[E.19]Fugas de información			10%			0,0	0,0	0,7	0,0	0,0
	[E.20]Vulnerabilidades de los programas	1%	20%	20%			0,1	1,8	1,4	0,0	0,0
	[E.21]Errores de mantenimiento\actualización de SW	1%	1%				0,1	0,1	0,0	0,0	0,0
	[E.24]Caída del sistema por agotamiento de recursos	50%					5,0	0,0	0,0	0,0	0,0
	[A.5]Suplantación de identidad		100%	100%	100%		0,0	9,0	7,0	9,0	0,0
	[A.7]Uso no previsto	10%	10%	10%			1,0	0,9	0,7	0,0	0,0
	[A.8]Difusión de software dañino	100%	100%	100%			10,0	9,0	7,0	0,0	0,0
	[A.9][Re-]encaminamiento de mensajes			10%			0,0	0,0	0,7	0,0	0,0
	[A.10]Alteración de secuencia		10%				0,0	0,9	0,0	0,0	0,0
	[A.11]Acceso no autorizado		10%	50%	100%		0,0	0,9	3,5	9,0	0,0
	[A.12]Análisis de tráfico			2%			0,0	0,0	0,1	0,0	0,0
	[A.13]Repudio (negación de actuaciones)					100%	0,0	0,0	0,0	0,0	8,0
	[A.14]Interceptación de información(escucha)			10%			0,0	0,0	0,7	0,0	0,0
	[A.15]Modificación de la información		50%				0,0	4,5	0,0	0,0	0,0
	[A.18]Destrucción de la información	50%					5,0	0,0	0,0	0,0	0,0
	[A.19]Revelación de información			50%			0,0	0,0	3,5	0,0	0,0
	[A.22]Manipulación de programas	50%	100%	100%			5,0	9,0	7,0	0,0	0,0
	[A.24]Denegación de servicio	100%					1,0	0,0	0,0	0,0	0,0
[B][S] Red Lan Operativa Voz y Datos											
	[I.8] Fallo de servicios de comunicaciones	50%					5,0	0,0	0,0	0,0	0,0
	[E.2]Errores del admin del sistema\de la seguridad	20%	20%	20%			2,0	2,0	0,0	0,0	0,0
	[E.9]Errores de [re-]encaminamiento			10%			0,0	0,0	0,0	0,0	0,0
	[E.10]Errores de secuencia		10%				0,0	1,0	0,0	0,0	0,0
	[E.15]Alteración de información		1%				0,0	0,1	0,0	0,0	0,0
	[E.19]Fugas de información			10%			0,0	0,0	0,0	0,0	0,0

Nombre	Amenaza	D	I	C	A	T	D	I	C	A	T
	[E.24]Caída del sistema por agotamiento de recursos	50%					5,0	0,0	0,0	0,0	0,0
	[A.5]Suplantación de identidad		10%	50%	100%		0,0	1,0	0,0	3,0	0,0
	[A.7]Uso no previsto	10%	10%	10%			1,0	1,0	0,0	0,0	0,0
	[A.9][Re-]encaminamiento de mensajes			10%			0,0	0,0	1,0	0,0	0,0
	[A.10]Alteración de secuencia		10%				0,0	1,0	0,0	0,0	0,0
	[A.11]Acceso no autorizado		10%	50%			0,0	1,0	0,0	0,0	0,0
	[A.12]Análisis de tráfico			2%	100%		0,0	0,0	0,2	3,0	0,0
	[A.14]Interceptación de información(escucha)			1%			0,0	0,0	0,1	0,0	0,0
	[A.15]Modificación de la información		10%				0,0	1,0	0,0	0,0	0,0
	[A.18]Destrucción de la información	50%					5,0	0,0	0,0	0,0	0,0
	[A.24]Denegación de servicio	50%					5,0	0,0	0,0	0,0	0,0
[B][S] Servicio de gestión de marcación telefónica											
	[I.5]Avería de origen físico o lógico	50%					5,0	0,0	0,0	0,0	0,0
	[E.8]Difusión de software Dañino	10%	10%	10%			1,0	1,0	0,9	0,0	0,0
	[E.20]Vulnerabilidades de los programas	1%	20%	20%			0,1	2,0	1,8	0,0	0,0
	[E.21]Errores de mantenimiento\actualización de SW	50%	50%				5,0	5,0	0,0	0,0	0,0
	[A.8]Difusión de software dañino	50%	50%	50%			5,0	5,0	4,5	0,0	0,0
	[A.22]Manipulación de programas	50%	100%	100%			5,0	10,0	9,0	0,0	0,0
[B][IS][D] Base de datos operativa											
	[E.3] Errores de monitorización (log)		10%				0,0	1,0	0,0	0,0	0,0
	[E.15]Alteración de información		50%				0,0	5,0	0,0	0,0	0,0
	[E.18]Destrucción de la información	100%					0,0	0,0	0,0	0,0	0,0
	[E.19]Fugas de información			100%			0,0	0,0	9,0	0,0	0,0
	[A.3]Manipulación de los registros de actividad (log)		30%				0,0	3,0	0,0	0,0	0,0
	[A.5]Suplantación de identidad		10%	100%	100%		0,0	1,0	9,0	3,0	0,0
	[A.6]Abuso de privilegios de acceso	1%	10%	50%			0,1	1,0	4,5	0,0	0,0
	[A.11]Acceso no autorizado		50%	100%			0,0	5,0	9,0	0,0	0,0
[A][P] Personal operativo											
	[E.15]Alteración de información		10%				0,0	0,7	0,0	0,0	0,0
	[E.18]Destrucción de la información	50%					3,5	0,0	0,0	0,0	0,0
	[E.19]Fugas de información			30%			0,0	0,0	2,1	0,0	0,0
	[E.28]Indisponibilidad del personal	30%					2,1	0,0	0,0	0,0	0,0
	[A.15]Modificación de la información		50%				0,0	3,5	0,0	0,0	0,0
	[A.18]Destrucción de la información	50%					3,5	0,0	0,0	0,0	0,0
	[A.19]Revelación de información			50%			0,0	0,0	3,5	0,0	0,0
	[A.28]Indisponibilidad del personal	30%					2,1	0,0	0,0	0,0	0,0
	[A.29]Extorsión	20%	20%	50%			1,4	1,4	3,5	0,0	0,0

Nombre	Amenaza	D	I	C	A	T	D	I	C	A	T
	[A.20]Ingeniería Social	1%	1%	50%			0,1	0,1	3,5	0,0	0,0
[A][P] Personal administrativo RRHH\Finanzas\Gerencia											
	[E.15]Alteración de información		10%				0,0	0,7	0,0	0,0	0,0
	[E.18]Destrucción de la información	1%					0,1	0,0	0,0	0,0	0,0
	[E.19]Fugas de información			30%			0,0	0,0	2,1	0,0	0,0
	[E.28]Indisponibilidad del personal	20%					1,4	0,0	0,0	0,0	0,0
	[A.15]Modificación de la información		100%				0,0	7,0	0,0	0,0	0,0
	[A.18]Destrucción de la información	10%					0,7	0,0	0,0	0,0	0,0
	[A.19]Revelación de información			50%			0,0	0,0	3,5	0,0	0,0
	[A.28]Indisponibilidad del personal	20%					1,4	0,0	0,0	0,0	0,0
	[A.29]Extorsión	20%	30%	50%			1,4	2,1	3,5	0,0	0,0
	[A.20]Ingeniería Social	10%	10%	100%			0,7	0,7	7,0	0,0	0,0
[A][P] Personal estructura operativa											
	[E.15]Alteración de información		10%				0,0	0,7	0,0	0,0	0,0
	[E.18]Destrucción de la información	1%					0,1	0,0	0,0	0,0	0,0
	[E.19]Fugas de información			70%			0,0	0,0	4,9	0,0	0,0
	[E.28]Indisponibilidad del personal	30%					2,1	0,0	0,0	0,0	0,0
	[A.15]Modificación de la información		50%				0,0	3,5	0,0	0,0	0,0
	[A.18]Destrucción de la información	10%					0,7	0,0	0,0	0,0	0,0
	[A.19]Revelación de información			70%			0,0	0,0	4,9	0,0	0,0
	[A.28]Indisponibilidad del personal	50%					3,5	0,0	0,0	0,0	0,0
	[A.29]Extorsión	20%	20%	50%			1,4	1,4	3,5	0,0	0,0
	[A.20]Ingeniería Social	10%	10%	100%			0,7	0,7	7,0	0,0	0,0
[A][L] Edificio General											
	[N.1]Fuego	100%					9,0				
	[N.2]Daños por agua	80%					7,2				
	[N.*]Desastres naturales	100%					9,0				
	[I.1]Fuego	100%					9,0				
	[I.2]Daños por agua	80%					7,2				
	[I.*]Desastres industriales	80%					7,2				
	[I.3]Contaminación medioambiental	10%					0,9				
	[I.4]Contaminación electromagnética	10%					0,9				
	[A.6]Abuso de privilegios de acceso	10%					0,9				
	[A.7]Uso no previsto	10%					0,9				
	[A.26]Ataque destructivo	100%					9,0				
	[A.27]Ocupación enemiga	100%					9,0				
[A][L] Centro de											
	[N.1]Fuego	100%					10,0				

Nombre	Amenaza	D	I	C	A	T	D	I	C	A	T
	[N.2]Daños por agua	100%					10,0				
	[N.*]Desastres naturales	100%					10,0				
	[I.1]Fuego	100%					10,0				
	[I.2]Daños por agua	100%					10,0				
	[I.*]Desastres industriales	100%					10,0				
	[I.3]Contaminación medioambiental	10%					1,0				
	[I.4]Contaminación electromagnética	40%					4,0				
	[A.6]Abuso de privilegios de acceso	100%					10,0				
	[A.7]Uso no previsto	10%					1,0				
	[A.26]Ataque destructivo	100%					10,0				
	[A.27]Ocupación enemiga	100%					10,0				
[A][L] Locaciones operativas y administrativas											
	[N.1]Fuego	100%					9,0				
	[N.2]Daños por agua	80%					7,2				
	[N.*]Desastres naturales	100%					9,0				
	[I.1]Fuego	100%					9,0				
	[I.2]Daños por agua	80%					7,2				
	[I.*]Desastres industriales	100%					9,0				
	[I.3]Contaminación medioambiental	10%					0,9				
	[I.4]Contaminación electromagnética	10%					0,9				
	[A.6]Abuso de privilegios de acceso	20%					1,8				
	[A.7]Uso no previsto	50%					4,5				
	[A.26]Ataque destructivo	100%					9,0				
	[A.27]Ocupación enemiga	100%					9,0				
[A][SS] Servicios generales mantenimiento											
	[E.15]Alteración de información						0,0				
	[E.18]Destrucción de la información	10%					0,4				
	[E.19]Fugas de información						0,0				
	[A.15]Modificación de la información						0,0				
	[A.18]Destrucción de la información	10%					0,4				
	[A.19]Revelación de información						0,0				
	[A.28]Indisponibilidad del personal	10%					0,4				
	[A.29]Extorsión	10%					0,4				
	[A.30]Ingeniería Social	10%					0,4				
[A][SS] Servicio de página web											
	[I.9]Interrupción de otros servicios o suministros esenciales	50%					2,5	0,0	0,0	0,0	0,0
	[E.15]Alteración de información		10%				0,0	0,5	0,0	0,0	0,0
	[E.18]Destrucción de la información	10%					0,5	0,0	0,0	0,0	0,0

Nombre	Amenaza	D	I	C	A	T	D	I	C	A	T
	[E.19]Fugas de información			10%			0,0	0,0	0,0	0,0	0,0
	[A.5]Suplantación de identidad		100%	50%	100%		0,0	5,0	0,0	0,0	0,0
	[A.13]Repudio (negación de actuaciones)					100%	0,0	0,0	0,0	0,0	1,0
	[A.15]Modificación de la información		50%				0,0	2,5	0,0	0,0	0,0
	[A.18]Destrucción de la información	50%					2,5	0,0	0,0	0,0	0,0
	[A.19]Revelación de información			50%			0,0	0,0	0,0	0,0	0,0
	[A.24]Denegación de servicio	100%					5,0	0,0	0,0	0,0	0,0
[A][SS] Servicio de correo electrónico											
	[I.9]Interrupción de otros servicios o suministros esenciales	50%					2,5	0,0	0,0	0,0	0,0
	[E.15]Alteración de información		10%				0,0	0,6	0,0	0,0	0,0
	[E.18]Destrucción de la información	10%					0,5	0,0	0,0	0,0	0,0
	[E.19]Fugas de información			10%			0,0	0,0	0,6	0,0	0,0
	[A.5]Suplantación de identidad		100%	100%	100%		0,0	6,0	6,0	5,0	0,0
	[A.13]Repudio (negación de actuaciones)					100%	0,0	0,0	0,0	0,0	0,0
	[A.15]Modificación de la información		50%				0,0	3,0	0,0	0,0	0,0
	[A.18]Destrucción de la información	50%					2,5	0,0	0,0	0,0	0,0
	[A.19]Revelación de información			50%			0,0	0,0	3,0	0,0	0,0
	[A.24]Denegación de servicio	50%					2,5	0,0	0,0	0,0	0,0
[A][SS] Servicio de líneas móviles											
	[I.8]Fallo de servicios de comunicaciones	50%					2,0	0,0	0,0	0,0	0,0
	[E.2]Errores del admin del sistema\de la seguridad	20%	20%	20%			0,8	0,6	0,6	0,0	0,0
	[E.9]Errores de [re-]encaminamiento			10%			0,0	0,0	0,3	0,0	0,0
	[E.10]Errores de secuencia		10%				0,0	0,3	0,0	0,0	0,0
	[E.15]Alteración de información		1%				0,0	0,0	0,0	0,0	0,0
	[E.19]Fugas de información			50%			0,0	0,0	1,5	0,0	0,0
	[E.24]Caída del sistema por agotamiento de recursos	50%					2,0	0,0	0,0	0,0	0,0
	[A.5]Suplantación de identidad		10%	50%	100%		0,0	0,3	1,5	0,0	0,0
	[A.7]Uso no previsto	10%	10%	10%			0,4	0,3	0,3	0,0	0,0
	[A.9][Re-]encaminamiento de mensajes			10%			0,0	0,0	0,3	0,0	0,0
	[A.10]Alteración de secuencia		10%				0,0	0,3	0,0	0,0	0,0
	[A.11]Acceso no autorizado		10%	50%	100%		0,0	0,3	1,5	0,0	0,0
	[A.12]Análisis de tráfico			2%			0,0	0,0	0,1	0,0	0,0
	[A.14]Interceptación de información(escucha)			10%			0,0	0,0	0,3	0,0	0,0
	[A.15]Modificación de la información		10%				0,0	0,3	0,0	0,0	0,0
	[A.18]Destrucción de la información	50%					2,0	0,0	0,0	0,0	0,0
	[A.24]Denegación de servicio	50%					2,0	0,0	0,0	0,0	0,0
[A][SW]											

Nombre	Amenaza	D	I	C	A	T	D	I	C	A	T
	[I.5]Avería de origen físico o lógico	50%					2,0	0,0	0,0	0,0	0,0
	[E.8]Difusión de software Dañino	10%	10%	10%			0,4	0,3	0,0	0,0	0,0
	[E.20]Vulnerabilidades de los programas	1%	20%	20%			0,0	0,6	0,0	0,0	0,0
	[E.21]Errores de mantenimiento\actualización de SW	1%	1%				0,0	0,0	0,0	0,0	0,0
	[A.8]Difusión de software dañino	50%	50%	50%			2,0	1,5	0,0	0,0	0,0
	[A.22]Manipulación de programas	50%	100%	100%			2,0	3,0	0,0	0,0	0,0
[A][SW] Software antivirus											
	[I.5]Avería de origen físico o lógico	50%					3,5	0,0	0,0	0,0	0,0
	[E.8]Difusión de software Dañino	10%	10%	10%			0,7	0,3	0,0	0,0	0,0
	[E.20]Vulnerabilidades de los programas	1%	20%	20%			0,1	0,6	0,0	0,0	0,0
	[E.21]Errores de mantenimiento\actualización de SW	1%	1%				0,1	0,0	0,0	0,0	0,0
	[A.8]Difusión de software dañino	100%	100%	100%			7,0	3,0	0,0	0,0	0,0
	[A.22]Manipulación de programas	50%	100%	100%			3,5	3,0	0,0	0,0	0,0
[A][SW] Software administrativo-contabilidad-rrhh											
	[I.5]Avería de origen físico o lógico	50%					4,5	0,0	0,0	0,0	0,0
	[E.8]Difusión de software Dañino	10%	10%	10%			0,9	0,7	0,8	0,0	0,0
	[E.20]Vulnerabilidades de los programas	1%	20%	20%			0,1	1,4	1,6	0,0	0,0
	[E.21]Errores de mantenimiento\actualización de SW	1%	1%				0,1	0,1	0,0	0,0	0,0
	[A.8]Difusión de software dañino	50%	50%	50%			4,5	3,5	4,0	0,0	0,0
	[A.22]Manipulación de programas	50%	100%	100%			4,5	7,0	8,0	0,0	0,0
[A][HW] Equipos de escritorio - laptops											
	[N.1]Fuego	100%					9,0	0,0	0,0	0,0	0,0
	[N.2]Daños por agua	30%					2,7	0,0	0,0	0,0	0,0
	[N.*]Desastres naturales	100%					9,0	0,0	0,0	0,0	0,0
	[I.1]Fuego	100%					9,0	0,0	0,0	0,0	0,0
	[I.2]Daños por agua	30%					2,7	0,0	0,0	0,0	0,0
	[I.*]Desastres industriales	100%					9,0	0,0	0,0	0,0	0,0
	[I.3]Contaminación medioambiental	10%					0,9	0,0	0,0	0,0	0,0
	[I.4]Contaminación electromagnética	10%					0,9	0,0	0,0	0,0	0,0
	[I.5]Avería de origen físico o lógico	50%					4,5	0,0	0,0	0,0	0,0
	[I.6]Corte del suministro eléctrico	100%					9,0	0,0	0,0	0,0	0,0
	[I.7]Condiciones Inadecuadas de temperatura o humedad	50%					4,5	0,0	0,0	0,0	0,0
	[I.11]Emanaciones electromagnéticas			1%			0,0	0,0	0,1	0,0	0,0
	[E.8]Difusión de software Dañino	30%	30%	30%			2,7	1,5	2,1	0,0	0,0
	[E.20]Vulnerabilidades de los programas	30%	30%	30%			2,7	1,5	2,1	0,0	0,0
	[E.21]Errores de mantenimiento\actualización de SW	30%	30%				2,7	1,5	0,0	0,0	0,0

Nombre	Amenaza	D	I	C	A	T	D	I	C	A	T
	[E.23]Errores de mantenimiento\actualización de HW	30%					2,7	0,0	0,0	0,0	0,0
	[E.24]Caída del sistema por agotamiento de recursos	50%					4,5	0,0	0,0	0,0	0,0
	[E.25]Pérdida de equipos	30%		30%			2,7	0,0	2,1	0,0	0,0
	[A.7]Uso no previsto	10%	1%	10%			0,9	0,1	0,7	0,0	0,0
	[A.8]Difusión de software dañino	30%	30%	30%			2,7	1,5	2,1	0,0	0,0
	[A.11]Acceso no autorizado	10%	10%	50%			0,9	0,5	3,5	0,0	0,0
	[A.22]Manipulación de programas	50%	100%	100%			4,5	5,0	7,0	0,0	0,0
	[A.23]Manipulación del hardware	50%		50%			4,5	0,0	3,5	0,0	0,0
	[A.24]Denegación de servicio	100%					9,0	0,0	0,0	0,0	0,0
	[A.25]Robo de equipos	50%		50%			4,5	0,0	3,5	0,0	0,0
	[A.26]Ataque destructivo	100%					9,0	0,0	0,0	0,0	0,0
[A][HW] Servidores											
	[N.1]Fuego	100%					10,0	0,0	0,0	0,0	0,0
	[N.2]Daños por agua	100%					10,0	0,0	0,0	0,0	0,0
	[N.*]Desastres naturales	100%					10,0	0,0	0,0	0,0	0,0
	[I.1]Fuego	100%					10,0	0,0	0,0	0,0	0,0
	[I.2]Daños por agua	100%					10,0	0,0	0,0	0,0	0,0
	[I.*]Desastres industriales	100%					10,0	0,0	0,0	0,0	0,0
	[I.3]Contaminación medioambiental	100%					10,0	0,0	0,0	0,0	0,0
	[I.4]Contaminación electromagnética	100%					10,0	0,0	0,0	0,0	0,0
	[I.5]Avería de origen físico o lógico	100%					10,0	0,0	0,0	0,0	0,0
	[I.6]Corte del suministro eléctrico	100%					10,0	0,0	0,0	0,0	0,0
	[I.7]Condiciones Inadecuadas de temperatura o humedad	100%					10,0	0,0	0,0	0,0	0,0
	[I.10]Degradación de los soportes de almacenamiento	100%					10,0	0,0	0,0	0,0	0,0
	[I.11]Emanaciones electromagnéticas			50%			0,0	0,0	4,5	0,0	0,0
	[E.1]Errores de los usuarios	100%	100%	100%			10,0	9,0	9,0	0,0	0,0
	[E.2]Errores del admin del sistema\de la seguridad	100%	100%	100%			10,0	9,0	9,0	0,0	0,0
	[E.3] Errores de monitorización (log)		50%				0,0	4,5	0,0	0,0	0,0
	[E.4]Errores de configuración		100%				0,0	9,0	0,0	0,0	0,0
	[E.8]Difusión de software Dañino	100%	100%	100%			10,0	9,0	9,0	0,0	0,0
	[E.15]Alteración de información		100%				0,0	9,0	0,0	0,0	0,0
	[E.18]Destrucción de la información	100%					10,0	0,0	0,0	0,0	0,0
	[E.19]Fugas de información			100%			0,0	0,0	9,0	0,0	0,0
	[E.20]Vulnerabilidades de los programas	50%	50%	50%			5,0	4,5	4,5	0,0	0,0
	[E.21]Errores de mantenimiento\actualización de SW	100%	50%				10,0	4,5	0,0	0,0	0,0

Nombre	Amenaza	D	I	C	A	T	D	I	C	A	T
	[E.23]Errores de mantenimiento\actualización de HW	100%					10,0	0,0	0,0	0,0	0,0
	[E.24]Caída del sistema por agotamiento de recursos	100%					10,0	0,0	0,0	0,0	0,0
	[E.25]Pérdida de equipos	100%		100%			10,0	0,0	9,0	0,0	0,0
	[A.3]Manipulación de los registros de actividad (log)		50%				0,0	4,5	0,0	0,0	0,0
	[A.4]Manipulación de los ficheros de configuración	100%	100%	100%			10,0	9,0	9,0	0,0	0,0
	[A.5]Suplantación de identidad		50%	100%	100%		0,0	4,5	9,0	10,0	0,0
	[A.6]Abuso de privilegios de acceso	1%	30%	100%	100%		0,1	2,7	9,0	10,0	0,0
	[A.7]Uso no previsto	1%	10%	10%			0,1	0,9	0,9	0,0	0,0
	[A.8]Difusión de software dañino	100%	100%	100%			10,0	9,0	9,0	0,0	0,0
	[A.11]Acceso no autorizado	10%	10%	50%	100%		1,0	0,9	4,5	10,0	0,0
	[A.13]Repudio (negación de actuaciones)					100%	0,0	0,0	0,0	0,0	7,0
	[A.15]Modificación de la información		100%				0,0	9,0	0,0	0,0	0,0
	[A.18]Destrucción de la información	100%					10,0	0,0	0,0	0,0	0,0
	[A.22]Manipulación de programas	100%	100%	100%			10,0	9,0	9,0	0,0	0,0
	[A.23]Manipulación del hardware	100%		50%			10,0	0,0	4,5	0,0	0,0
	[A.24]Denegación de servicio	100%					10,0	0,0	0,0	0,0	0,0
	[A.25]Robo de equipos	100%		100%			10,0	0,0	9,0	0,0	0,0
	[A.26]Ataque destructivo	100%					10,0	0,0	0,0	0,0	0,0
[A][HW] Equipos de telefonía móvil											
	[N.1]Fuego	100%					5,0	0,0	0,0	0,0	0,0
	[N.2]Daños por agua	100%					5,0	0,0	0,0	0,0	0,0
	[N.*]Desastres naturales	100%					5,0	0,0	0,0	0,0	0,0
	[I.1]Fuego	100%					5,0	0,0	0,0	0,0	0,0
	[I.2]Daños por agua	100%					5,0	0,0	0,0	0,0	0,0
	[I.*]Desastres industriales	100%					5,0	0,0	0,0	0,0	0,0
	[I.3]Contaminación medioambiental	10%					0,5	0,0	0,0	0,0	0,0
	[I.4]Contaminación electromagnética	10%					0,5	0,0	0,0	0,0	0,0
	[I.5]Avería de origen físico o lógico	50%					2,5	0,0	0,0	0,0	0,0
	[I.6]Corte del suministro eléctrico	10%					0,5	0,0	0,0	0,0	0,0
	[I.7]Condiciones Inadecuadas de temperatura o humedad	30%					1,5	0,0	0,0	0,0	0,0
	[I.11]Emanaciones electromagnéticas			1%			0,0	0,0	0,1	0,0	0,0
	[E.8]Difusión de software Dañino	30%	20%	20%			1,5	0,8	1,0	0,0	0,0
	[E.20]Vulnerabilidades de los programas	30%	20%	20%			1,5	0,8	1,0	0,0	0,0
	[E.21]Errores de mantenimiento\actualización de SW	30%	20%				1,5	0,8	0,0	0,0	0,0
	[E.23]Errores de mantenimiento\actualización de HW	30%					1,5	0,0	0,0	0,0	0,0

Nombre	Amenaza	D	I	C	A	T	D	I	C	A	T
	[E.24]Caída del sistema por agotamiento de recursos	100%					5,0	0,0	0,0	0,0	0,0
	[E.25]Pérdida de equipos	100%		20%			5,0	0,0	1,0	0,0	0,0
	[A.7]Uso no previsto	10%	10%	10%			0,5	0,4	0,5	0,0	0,0
	[A.8]Difusión de software dañino	30%	20%	20%			1,5	0,8	1,0	0,0	0,0
	[A.11]Acceso no autorizado	10%	10%	20%			0,5	0,4	1,0	0,0	0,0
	[A.22]Manipulación de programas	30%	20%	20%			1,5	0,8	1,0	0,0	0,0
	[A.23]Manipulación del hardware	50%		10%			2,5	0,0	0,5	0,0	0,0
	[A.24]Denegación de servicio	100%					5,0	0,0	0,0	0,0	0,0
	[A.25]Robo de equipos	100%		20%			5,0	0,0	1,0	0,0	0,0
	[A.26]Ataque destructivo	100%					5,0	0,0	0,0	0,0	0,0
[A][AUX] Sistema de alimentación ininterrumpido	Valoración General										
	[N.1]Fuego	100%					10,0	0,0	0,0	0,0	0,0
	[N.2]Daños por agua	100%					10,0	0,0	0,0	0,0	0,0
	[N.*]Desastres naturales	100%					10,0	0,0	0,0	0,0	0,0
	[I.1]Fuego	100%					10,0	0,0	0,0	0,0	0,0
	[I.2]Daños por agua	100%					10,0	0,0	0,0	0,0	0,0
	[I.*]Desastres industriales	100%					10,0	0,0	0,0	0,0	0,0
	[I.3]Contaminación medioambiental	50%					5,0	0,0	0,0	0,0	0,0
	[E.23]Errores de mantenimiento\actualización de HW	50%					5,0	0,0	0,0	0,0	0,0
	[A.7]Uso no previsto	50%					5,0	0,0	0,0	0,0	0,0
	[A.23]Manipulación del hardware	50%					5,0	0,0	0,0	0,0	0,0
	[A.25]Robo de equipos	100%					10,0	0,0	0,0	0,0	0,0
	[A.26]Ataque destructivo	100%					10,0	0,0	0,0	0,0	0,0
[A][AUX] Generador eléctrico de respaldo											
	[N.1]Fuego	100%					9,0	0,0	0,0	0,0	0,0
	[N.2]Daños por agua	100%					9,0	0,0	0,0	0,0	0,0
	[N.*]Desastres naturales	100%					9,0	0,0	0,0	0,0	0,0
	[I.1]Fuego	100%					9,0	0,0	0,0	0,0	0,0
	[I.2]Daños por agua	100%					9,0	0,0	0,0	0,0	0,0
	[I.*]Desastres industriales	100%					9,0	0,0	0,0	0,0	0,0
	[I.3]Contaminación medioambiental	50%					4,5	0,0	0,0	0,0	0,0
	[E.23]Errores de mantenimiento\actualización de HW	50%					4,5	0,0	0,0	0,0	0,0
	[A.7]Uso no previsto	50%					4,5	0,0	0,0	0,0	0,0
	[A.23]Manipulación del hardware	50%					4,5	0,0	0,0	0,0	0,0
	[A.25]Robo de equipos	100%					9,0	0,0	0,0	0,0	0,0
	[A.26]Ataque destructivo	100%					9,0	0,0	0,0	0,0	0,0

Nombre	Amenaza	D	I	C	A	T	D	I	C	A	T
[A][AUX] Cableado eléctrico Centro											
	[N.1]Fuego	100%					9,0	0,0	0,0	0,0	0,0
	[N.2]Daños por agua	50%					4,5	0,0	0,0	0,0	0,0
	[N.*]Desastres naturales	100%					9,0	0,0	0,0	0,0	0,0
	[I.1]Fuego	100%					9,0	0,0	0,0	0,0	0,0
	[I.2]Daños por agua	50%					4,5	0,0	0,0	0,0	0,0
	[I.*]Desastres industriales	100%					9,0	0,0	0,0	0,0	0,0
	[I.3]Contaminación medioambiental	30%					2,7	0,0	0,0	0,0	0,0
	[I.4]Contaminación electromagnética	30%					2,7	0,0	0,0	0,0	0,0
	[I.11]Emanaciones electromagnéticas			0%			0,0	0,0	0,0	0,0	0,0
	[E.23]Errores de mantenimiento\actualización de HW	30%					2,7	0,0	0,0	0,0	0,0
	[A.7]Uso no previsto	30%	1%	0%			2,7	0,0	0,0	0,0	0,0
	[A.11]Acceso no autorizado		1%	0%			0,0	0,0	0,0	0,0	0,0
	[A.23]Manipulación del hardware	50%		0%			4,5	0,0	0,0	0,0	0,0
	[A.25]Robo de equipos	100%		0%			9,0	0,0	0,0	0,0	0,0
	[A.26]Ataque destructivo	100%					9,0	0,0	0,0	0,0	0,0
[A][AUX] Cableado fibra óptica											
	[N.1]Fuego	100%					9,0	0,0	0,0	0,0	0,0
	[N.2]Daños por agua	50%					4,5	0,0	0,0	0,0	0,0
	[N.*]Desastres naturales	100%					9,0	0,0	0,0	0,0	0,0
	[I.1]Fuego	100%					9,0	0,0	0,0	0,0	0,0
	[I.2]Daños por agua	50%					4,5	0,0	0,0	0,0	0,0
	[I.*]Desastres industriales	100%					9,0	0,0	0,0	0,0	0,0
	[I.3]Contaminación medioambiental	50%					4,5	0,0	0,0	0,0	0,0
	[E.23]Errores de mantenimiento\actualización de HW	100%					9,0	0,0	0,0	0,0	0,0
	[A.7]Uso no previsto	50%	30%	30%			4,5	0,0	0,0	0,0	0,0
	[A.23]Manipulación del hardware	100%		50%			9,0	0,0	0,0	0,0	0,0
	[A.25]Robo de equipos	100%		0%			9,0	0,0	0,0	0,0	0,0
	[A.26]Ataque destructivo	100%					9,0	0,0	0,0	0,0	0,0
[A][AUX] Impresoras Operativas y Administrativas											
	[N.1]Fuego	100%					2,0	0,0	0,0	0,0	0,0
	[N.2]Daños por agua	50%					1,0	0,0	0,0	0,0	0,0
	[N.*]Desastres naturales	100%					2,0	0,0	0,0	0,0	0,0
	[I.1]Fuego	100%					2,0	0,0	0,0	0,0	0,0
	[I.2]Daños por agua	50%					1,0	0,0	0,0	0,0	0,0
	[I.*]Desastres industriales	100%					2,0	0,0	0,0	0,0	0,0
	[I.3]Contaminación medioambiental	50%					1,0	0,0	0,0	0,0	0,0
	[I.4]Contaminación electromagnética	10%					0,2	0,0	0,0	0,0	0,0

Nombre	Amenaza	D	I	C	A	T	D	I	C	A	T
	[I.5]Avería de origen físico o lógico	100%					2,0	0,0	0,0	0,0	0,0
	[I.6]Corte del suministro eléctrico	100%					2,0	0,0	0,0	0,0	0,0
	[I.7]Condiciones Inadecuadas de temperatura o humedad	100%					2,0	0,0	0,0	0,0	0,0
	[I.11]Emanaciones electromagnéticas			1%			0,0	0,0	0,0	0,0	0,0
	[E.23]Errores de mantenimiento\actualización de HW	50%					1,0	0,0	0,0	0,0	0,0
	[E.24]Caída del sistema por agotamiento de recursos	50%					1,0	0,0	0,0	0,0	0,0
	[E.25]Pérdida de equipos	100%		50%			2,0	0,0	0,0	0,0	0,0
	[A.11]Acceso no autorizado	10%	10%	50%			0,2	0,0	0,0	0,0	0,0
	[A.23]Manipulación del hardware	100%		50%			2,0	0,0	0,0	0,0	0,0
	[A.24]Denegación de servicio	100%					2,0	0,0	0,0	0,0	0,0
	[A.25]Robo de equipos	100%		50%			2,0	0,0	0,0	0,0	0,0
	[A.26]Ataque destructivo	100%					2,0	0,0	0,0	0,0	0,0
[A][AUX] Servicio Backups											
	[N.1]Fuego	100%					9,0	0,0	0,0	0,0	0,0
	[N.2]Daños por agua	100%					9,0	0,0	0,0	0,0	0,0
	[N.*]Desastres naturales	100%					9,0	0,0	0,0	0,0	0,0
	[I.1]Fuego	100%					9,0	0,0	0,0	0,0	0,0
	[I.2]Daños por agua	100%					9,0	0,0	0,0	0,0	0,0
	[I.*]Desastres industriales	100%					9,0	0,0	0,0	0,0	0,0
	[I.3]Contaminación medioambiental	50%					4,5	0,0	0,0	0,0	0,0
	[I.4]Contaminación electromagnética	100%					9,0	0,0	0,0	0,0	0,0
	[I.5]Avería de origen físico o lógico	100%					9,0	0,0	0,0	0,0	0,0
	[I.6]Corte del suministro eléctrico	100%					9,0	0,0	0,0	0,0	0,0
	[I.7]Condiciones Inadecuadas de temperatura o humedad	100%					9,0	0,0	0,0	0,0	0,0
	[I.10]Degradación de los soportes de almacenamiento	100%					9,0	0,0	0,0	0,0	0,0
	[I.11]Emanaciones electromagnéticas			1%			0,0	0,0	0,1	0,0	0,0
	[E.1]Errores de los usuarios	50%	50%	50%			4,5	4,5	4,5	0,0	0,0
	[E.2]Errores del admin del sistema\de la seguridad	50%	50%	50%			4,5	4,5	4,5	0,0	0,0
	[E.15]Alteración de información		50%				0,0	4,5	0,0	0,0	0,0
	[E.18]Destrucción de la información	100%					9,0	0,0	0,0	0,0	0,0
	[E.19]Fugas de información			100%			0,0	0,0	9,0	0,0	0,0
	[E.23]Errores de mantenimiento\actualización de HW	100%					9,0	0,0	0,0	0,0	0,0
	[E.24]Caída del sistema por agotamiento de recursos	100%					9,0	0,0	0,0	0,0	0,0
	[E.25]Pérdida de equipos	100%		100%			9,0	0,0	9,0	0,0	0,0
	[A.5]Suplantación de identidad		50%	50%	100%		0,0	4,5	4,5	9,0	0,0

Nombre	Amenaza	D	I	C	A	T	D	I	C	A	T
	[A.6]Abuso de privilegios de acceso	1%	50%	100%	100%		0,1	4,5	9,0	9,0	0,0
	[A.7]Uso no previsto	1%	10%	10%			0,1	0,9	0,9	0,0	0,0
	[A.11]Acceso no autorizado		50%	100%	100%		0,0	4,5	9,0	9,0	0,0
	[A.13]Repudio (negación de actuaciones)					100%	0,0	0,0	0,0	0,0	9,0
	[A.15]Modificación de la información		100%				0,0	9,0	0,0	0,0	0,0
	[A.18]Destrucción de la información	100%					9,0	0,0	0,0	0,0	0,0
	[A.23]Manipulación del hardware	50%		50%			4,5	0,0	4,5	0,0	0,0
	[A.24]Denegación de servicio	50%					4,5	0,0	0,0	0,0	0,0
	[A.25]Robo de equipos	100%		100%			9,0	0,0	9,0	0,0	0,0
	[A.26]Ataque destructivo	100%					9,0	0,0	0,0	0,0	0,0
[A][COM] Switches Core y Distribuidores											
	[N.1]Fuego	100%					9,0	0,0	0,0	0,0	0,0
	[N.2]Daños por agua	100%					9,0	0,0	0,0	0,0	0,0
	[N.*]Desastres naturales	100%					9,0	0,0	0,0	0,0	0,0
	[I.1]Fuego	100%					9,0	0,0	0,0	0,0	0,0
	[I.2]Daños por agua	100%					9,0	0,0	0,0	0,0	0,0
	[I.*]Desastres industriales	100%					9,0	0,0	0,0	0,0	0,0
	[I.3]Contaminación medioambiental	50%					4,5	0,0	0,0	0,0	0,0
	[I.4]Contaminación electromagnética	50%					4,5	0,0	0,0	0,0	0,0
	[I.5]Avería de origen físico o lógico	100%					9,0	0,0	0,0	0,0	0,0
	[I.6]Corte del suministro eléctrico	100%					9,0	0,0	0,0	0,0	0,0
	[I.7]Condiciones Inadecuadas de temperatura o humedad	100%					9,0	0,0	0,0	0,0	0,0
	[I.11]Emanaciones electromagnéticas			1%			0,0	0,0	0,0	0,0	0,0
	[E.23]Errores de mantenimiento\actualización de HW	50%					4,5	0,0	0,0	0,0	0,0
	[E.24]Caída del sistema por agotamiento de recursos	50%					4,5	0,0	0,0	0,0	0,0
	[E.25]Pérdida de equipos	100%		10%			9,0	0,0	0,0	0,0	0,0
	[A.7]Uso no previsto	50%		10%			4,5	0,0	0,0	0,0	0,0
	[A.11]Acceso no autorizado	50%	10%	10%			4,5	0,0	0,0	0,0	0,0
	[A.23]Manipulación del hardware	100%		10%			9,0	0,0	0,0	0,0	0,0
	[A.24]Denegación de servicio	100%					9,0	0,0	0,0	0,0	0,0
	[A.25]Robo de equipos	100%		10%			9,0	0,0	0,0	0,0	0,0
	[A.26]Ataque destructivo	100%					9,0	0,0	0,0	0,0	0,0
[A][COM] Firewall											
	[N.1]Fuego	100%					10,0	0,0	0,0	0,0	0,0
	[N.2]Daños por agua	100%					10,0	0,0	0,0	0,0	0,0
	[N.*]Desastres naturales	100%					10,0	0,0	0,0	0,0	0,0
	[I.1]Fuego	100%					10,0	0,0	0,0	0,0	0,0

Nombre	Amenaza	D	I	C	A	T	D	I	C	A	T
	[I.2]Daños por agua	100%					10,0	0,0	0,0	0,0	0,0
	[I.*]Desastres industriales	100%					10,0	0,0	0,0	0,0	0,0
	[I.3]Contaminación medioambiental	50%					5,0	0,0	0,0	0,0	0,0
	[I.4]Contaminación electromagnética	50%					5,0	0,0	0,0	0,0	0,0
	[I.5]Avería de origen físico o lógico	100%					10,0	0,0	0,0	0,0	0,0
	[I.6]Corte del suministro eléctrico	100%					10,0	0,0	0,0	0,0	0,0
	[I.7]Condiciones Inadecuadas de temperatura o humedad	100%					10,0	0,0	0,0	0,0	0,0
	[I.11]Emanaciones electromagnéticas			1%			0,0	0,0	0,1	0,0	0,0
	[E.8]Difusión de software Dañino	100%	30%	30%			10,0	0,9	2,1	0,0	0,0
	[E.20]Vulnerabilidades de los programas	50%	20%	30%			5,0	0,6	2,1	0,0	0,0
	[E.21]Errores de mantenimiento\actualización de SW	100%	20%				10,0	0,6	0,0	0,0	0,0
	[E.23]Errores de mantenimiento\actualización de HW	100%					10,0	0,0	0,0	0,0	0,0
	[E.24]Caída del sistema por agotamiento de recursos	100%					10,0	0,0	0,0	0,0	0,0
	[E.25]Pérdida de equipos	100%		30%			10,0	0,0	2,1	0,0	0,0
	[A.7]Uso no previsto	50%		30%			5,0	0,0	2,1	0,0	0,0
	[A.8]Difusión de software dañino	50%	30%	30%			5,0	0,9	2,1	0,0	0,0
	[A.11]Acceso no autorizado	50%	20%	30%			5,0	0,6	2,1	0,0	0,0
	[A.22]Manipulación de programas	50%	20%	30%			5,0	0,6	2,1	0,0	0,0
	[A.23]Manipulación del hardware	100%		30%			10,0	0,0	2,1	0,0	0,0
	[A.24]Denegación de servicio	100%					10,0	0,0	0,0	0,0	0,0
	[A.25]Robo de equipos	100%		30%			10,0	0,0	2,1	0,0	0,0
	[A.26]Ataque destructivo	100%					10,0	0,0	0,0	0,0	0,0
[A][COM] Canal de internet principal y backup											
	[I.8]Fallo de servicios de comunicaciones	100%					7,0	0,0	0,0	0,0	0,0
	[E.2]Errores del administrador del sistema\de la seguridad	50%	50%	30%			3,5	3,5	0,9	0,0	0,0
	[E.9]Errores de [re-]encaminamiento			50%			0,0	0,0	1,5	0,0	0,0
	[E.10]Errores de secuencia		50%				0,0	3,5	0,0	0,0	0,0
	[E.15]Alteración de información		50%				0,0	3,5	0,0	0,0	0,0
	[E.18]Destrucción de la información	10%					0,7	0,0	0,0	0,0	0,0
	[E.19]Fugas de información			50%			0,0	0,0	1,5	0,0	0,0
	[E.24]Caída del sistema por agotamiento de recursos	100%					7,0	0,0	0,0	0,0	0,0
	[A.5]Suplantación de identidad		50%	50%	100%		0,0	3,5	1,5	3,0	0,0
	[A.7]Uso no previsto	50%	10%	10%			3,5	0,7	0,3	0,0	0,0
	[A.9][Re-]encaminamiento de mensajes			50%			0,0	0,0	1,5	0,0	0,0
	[A.10]Alteración de secuencia		50%				0,0	3,5	0,0	0,0	0,0
	[A.11]Acceso no autorizado		10%	50%	100%		0,0	0,7	1,5	3,0	0,0

Nombre	Amenaza	D	I	C	A	T	D	I	C	A	T
	[A.12]Análisis de tráfico			50%			0,0	0,0	1,5	0,0	0,0
	[A.13]Repudio (negación de actuaciones)					100%	0,0	0,0	0,0	0,0	3,0
	[A.14]Interceptación de información(escucha)			50%			0,0	0,0	1,5	0,0	0,0
	[A.15]Modificación de la información		50%				0,0	3,5	0,0	0,0	0,0
	[A.18]Destrucción de la información	10%					0,7	0,0	0,0	0,0	0,0
	[A.19]Revelación de información			50%			0,0	0,0	1,5	0,0	0,0
	[A.24]Denegación de servicio	100%					7,0	0,0	0,0	0,0	0,0
[A][COM] Canal de MPLS casa matriz Ppal y BCK											
	[I.8]Fallo de servicios de comunicaciones	100%					7,0	0,0	0,0	0,0	0,0
	[E.2]Errores del administrador del sistema\de la seguridad	50%	50%	30%			3,5	3,5	2,1	0,0	0,0
	[E.9]Errores de [re-]encaminamiento			50%			0,0	0,0	3,5	0,0	0,0
	[E.10]Errores de secuencia		50%				0,0	3,5	0,0	0,0	0,0
	[E.15]Alteración de información		50%				0,0	3,5	0,0	0,0	0,0
	[E.18]Destrucción de la información	10%					0,7	0,0	0,0	0,0	0,0
	[E.19]Fugas de información			50%			0,0	0,0	3,5	0,0	0,0
	[E.24]Caída del sistema por agotamiento de recursos	100%					7,0	0,0	0,0	0,0	0,0
	[A.5]Suplantación de identidad		50%	50%	100%		0,0	3,5	3,5	7,0	0,0
	[A.7]Uso no previsto	50%	10%	10%			3,5	0,7	0,7	0,0	0,0
	[A.9][Re-]encaminamiento de mensajes			50%			0,0	0,0	3,5	0,0	0,0
	[A.10]Alteración de secuencia		50%				0,0	3,5	0,0	0,0	0,0
	[A.11]Acceso no autorizado		10%	50%	100%		0,0	0,7	3,5	7,0	0,0
	[A.12]Análisis de tráfico			50%			0,0	0,0	3,5	0,0	0,0
	[A.13]Repudio (negación de actuaciones)					100%	0,0	0,0	0,0	0,0	7,0
	[A.14]Interceptación de información(escucha)			50%			0,0	0,0	3,5	0,0	0,0
	[A.15]Modificación de la información		50%				0,0	3,5	0,0	0,0	0,0
	[A.18]Destrucción de la información	10%					0,7	0,0	0,0	0,0	0,0
	[A.19]Revelación de información			50%			0,0	0,0	3,5	0,0	0,0
	[A.24]Denegación de servicio	100%					7,0	0,0	0,0	0,0	0,0
[A][COM] Cableado estructura voz y datos											
	[I.8]Fallo de servicios de comunicaciones	100%					9,0	0,0	0,0	0,0	0,0
	[E.2]Errores del administrador del sistema\de la seguridad	50%	50%	20%			4,5	3,5	1,4	0,0	0,0
	[E.9]Errores de [re-]encaminamiento			10%			0,0	0,0	0,7	0,0	0,0
	[E.10]Errores de secuencia		30%				0,0	2,1	0,0	0,0	0,0
	[E.15]Alteración de información		30%				0,0	2,1	0,0	0,0	0,0
	[E.19]Fugas de información			100%			0,0	0,0	7,0	0,0	0,0
	[E.24]Caída del sistema por agotamiento de recursos	100%					9,0	0,0	0,0	0,0	0,0

Nombre	Amenaza	D	I	C	A	T	D	I	C	A	T
	[A.5]Suplantación de identidad		10%	50%	100%		0,0	0,7	3,5	7,0	0,0
	[A.7]Uso no previsto	10%	10%	10%			0,9	0,7	0,7	0,0	0,0
	[A.9][Re-]encaminamiento de mensajes			10%			0,0	0,0	0,7	0,0	0,0
	[A.10]Alteración de secuencia		10%				0,0	0,7	0,0	0,0	0,0
	[A.11]Acceso no autorizado		10%	50%	100%		0,0	0,7	3,5	7,0	0,0
	[A.12]Análisis de tráfico			2%			0,0	0,0	0,1	0,0	0,0
	[A.14]Interceptación de información(escucha)			1%			0,0	0,0	0,1	0,0	0,0
	[A.15]Modificación de la información		10%				0,0	0,7	0,0	0,0	0,0
	[A.18]Destrucción de la información	50%					4,5	0,0	0,0	0,0	0,0
	[A.24]Denegación de servicio	100%					9,0	0,0	0,0	0,0	0,0
[A][IS] Serv. Tec. Aux. Ficheros configuración											
	[E.4]Errores de configuración		50%				0,0	1,5	0,0	0,0	0,0
	[E.15]Alteración de información		100%				0,0	3,0	0,0	0,0	0,0
	[E.18]Destrucción de la información	100%					5,0	0,0	0,0	0,0	0,0
	[E.19]Fugas de información			50%			0,0	0,0	2,5	0,0	0,0
	[A.4]Manipulación de los ficheros de configuración	30%	50%	50%			1,5	1,5	2,5	0,0	0,0
	[A.5]Suplantación de identidad		10%	50%	100%		0,0	0,3	2,5	0,0	0,0
	[A.6]Abuso de privilegios de acceso	1%	10%	50%			0,1	0,3	2,5	0,0	0,0
	[A.11]Acceso no autorizado		10%	50%			0,0	0,3	2,5	0,0	0,0
[A][IS] Serv. Tec. Aux. Manuales y Procedimientos											
	[E.4]Errores de configuración		50%				0,0	1,5	0,0	0,0	0,0
	[E.15]Alteración de información		100%				0,0	3,0	0,0	0,0	0,0
	[E.18]Destrucción de la información	100%					5,0	0,0	0,0	0,0	0,0
	[E.19]Fugas de información			50%			0,0	0,0	2,5	0,0	0,0
	[A.4]Manipulación de los ficheros de configuración	30%	50%	50%			1,5	1,5	2,5	0,0	0,0
	[A.5]Suplantación de identidad		10%	50%	100%		0,0	0,3	2,5	0,0	0,0
	[A.6]Abuso de privilegios de acceso	1%	10%	50%			0,1	0,3	2,5	0,0	0,0
	[A.11]Acceso no autorizado		10%	50%			0,0	0,3	2,5	0,0	0,0
[A][IS] Servicio de servidor de archivos											
	[E.1]Errores de los usuarios	20%	30%	10%			1,4	2,1	0,7	0,0	0,0
	[E.2]Errores del administrador del sistema\de la seguridad	50%	50%	20%			3,5	3,5	1,4	0,0	0,0
	[E.15]Alteración de información		50%				0,0	3,5	0,0	0,0	0,0
	[E.18]Destrucción de la información	100%					7,0	0,0	0,0	0,0	0,0
	[E.19]Fugas de información			100%			0,0	0,0	7,0	0,0	0,0
	[E.24]Caída del sistema por agotamiento de recursos	100%					7,0	0,0	0,0	0,0	0,0
	[A.5]Suplantación de identidad		50%	50%	100%		0,0	3,5	3,5	7,0	0,0

Nombre	Amenaza	D	I	C	A	T	D	I	C	A	T
	[A.6]Abuso de privilegios de acceso	1%	10%	50%	100%		0,1	0,7	3,5	7,0	0,0
	[A.7]Uso no previsto	20%	10%	10%			1,4	0,7	0,7	0,0	0,0
	[A.11]Acceso no autorizado		10%	50%	100%		0,0	0,7	3,5	7,0	0,0
	[A.13]Repudio (negación de actuaciones)					100%	0,0	0,0	0,0	0,0	7,0
	[A.15]Modificación de la información		50%				0,0	3,5	0,0	0,0	0,0
	[A.18]Destrucción de la información	100%					7,0	0,0	0,0	0,0	0,0
	[A.24]Denegación de servicio	100%					7,0	0,0	0,0	0,0	0,0
[A][IS] Servicio de base de datos administrativa											
	[E.1]Errores de los usuarios	10%	20%	10%			0,7	1,4	0,7	0,0	0,0
	[E.2]Errores del administrador del sistema\de la seguridad	100%	30%	20%			7,0	2,1	1,4	0,0	0,0
	[E.15]Alteración de información		50%				0,0	3,5	0,0	0,0	0,0
	[E.18]Destrucción de la información	100%	50%				7,0	0,0	0,0	0,0	0,0
	[E.19]Fugas de información			50%			0,0	0,0	3,5	0,0	0,0
	[E.24]Caída del sistema por agotamiento de recursos	100%					7,0	0,0	0,0	0,0	0,0
	[A.5]Suplantación de identidad		50%	50%	100%		0,0	3,5	3,5	7,0	0,0
	[A.6]Abuso de privilegios de acceso	1%	10%	50%	100%		0,1	0,7	3,5	7,0	0,0
	[A.7]Uso no previsto	1%	10%	50%			0,1	0,7	3,5	0,0	0,0
	[A.11]Acceso no autorizado		50%	50%	100%		0,0	3,5	3,5	7,0	0,0
	[A.13]Repudio (negación de actuaciones)					100%	0,0	0,0	0,0	0,0	7,0
	[A.15]Modificación de la información		50%				0,0	3,5	0,0	0,0	0,0
	[A.18]Destrucción de la información	100%					7,0	0,0	0,0	0,0	0,0
	[A.24]Denegación de servicio	100%					7,0	0,0	0,0	0,0	0,0

Fuente**:** Propia

8.2 RIESGOS

El cálculo del valor del impacto (en cada dominio del activo) y la definición de la frecuencia para cada amenaza del activo permite calcular el riesgo de forma directa (riesgo = impacto * frecuencia), considerando lo siguiente:

- El valor total del riesgo para cada dominio se obtiene del promedio de todas las amenazas en el dominio (para ese activo).

- El valor total del riesgo se obtiene del máximo valor obtenido del total del riesgo para cada dominio.

Para darle el nivel o valoración del riesgo se parte de la siguiente tabla (basada en la clasificación de la herramienta PILAR):

Cuadro 11. Clasificación del Riesgo

Valor Riesgo	Nivel Riesgo
>=9	Catástrofe
>=8	Desastre
>=7	Extremadamente Crítico
>=6	Muy Crítico
>=5	Crítico
>=4	Muy Alto
>=3	Alto
>=2	Medio
>=1	Bajo
>=0	Despreciable

Fuente: Propia

El resultado final del cálculo del riesgo se presenta en la siguiente tabla:

Cuadro 12. Cálculo del riesgo

Nom	Amenaza	Frec	D	I	C	A	T	Riesgo	Valoración
[B][S]Servicio Telefonía	Riesgo Total		10,82	9,98	7,55	9,00	8,00	10,82	Catástrofe
	[I.5]Avería de origen físico o lógico	1,00	5,0	0,0	0,0	0,0	0,0	5,0	Crítico
	[I.8]Fallo de servicios de comunicaciones	1,00	10,0	0,0	0,0	0,0	0,0	10,0	Catástrofe
	[E.2]Errores del administrador del sistema\de la seguridad	1,00	2,0	1,8	1,4	0,0	0,0	2,0	Medio
	[E.8]Difusión de software Dañino	1,00	1,0	0,9	0,7	0,0	0,0	1,0	Bajo
	[E.9]Errores de [re-]encaminamiento	1,00	0,0	0,0	0,7	0,0	0,0	0,7	Despreciable
	[E.10]Errores de secuencia	1,00	0,0	0,9	0,0	0,0	0,0	0,9	Despreciable
	[E.15]Alteración de información	1,00	0,0	0,9	0,0	0,0	0,0	0,9	Despreciable
	[E.18]Destrucción de la información	1,00	1,0	0,0	0,0	0,0	0,0	1,0	Bajo
	[E.19]Fugas de información	1,00	0,0	0,0	0,7	0,0	0,0	0,7	Despreciable
	[E.20]Vulnerabilidades de los programas	1,00	0,1	1,8	1,4	0,0	0,0	1,8	Bajo
	[E.21]Errores de mantenimiento\actualización de SW	1,00	0,1	0,1	0,0	0,0	0,0	0,1	Despreciable
	[E.24]Caída del sistema por agotamiento de recursos	0,10	0,5	0,0	0,0	0,0	0,0	0,5	Despreciable
	[A.5]Suplantación de identidad	1,00	0,0	9,0	7,0	9,0	0,0	9,0	Catástrofe
	[A.7]Uso no previsto	10,00	10,0	9,0	7,0	0,0	0,0	10,0	Catástrofe

Nom	Amenaza	Frec	D	I	C	A	T	Riesgo	Valoración
	[A.8]Difusión de software dañino	10,00	100,0	90,0	70,0	0,0	0,0	100,0	Catástrofe
	[A.9][Re-]encaminamiento de mensajes	1,00	0,0	0,0	0,7	0,0	0,0	0,7	Despreciable
	[A.10]Alteración de secuencia	1,00	0,0	0,9	0,0	0,0	0,0	0,9	Despreciable
	[A.11]Acceso no autorizado	1,00	0,0	0,9	3,5	9,0	0,0	9,0	Catástrofe
	[A.12]Análisis de tráfico	10,00	0,0	0,0	1,4	0,0	0,0	1,4	Bajo
	[A.13]Repudio (negación de actuaciones)	1,00	0,0	0,0	0,0	0,0	8,0	8,0	Desastre
	[A.14]Interceptación de información(escucha)	1,00	0,0	0,0	0,7	0,0	0,0	0,7	Despreciable
	[A.15]Modificación de la información	1,00	0,0	4,5	0,0	0,0	0,0	4,5	Muy Alto
	[A.18]Destrucción de la información	1,00	5,0	0,0	0,0	0,0	0,0	5,0	Crítico
	[A.19]Revelación de información	1,00	0,0	0,0	3,5	0,0	0,0	3,5	Alto
	[A.22]Manipulación de programas	1,00	5,0	9,0	7,0	0,0	0,0	9,0	Catástrofe
	[A.24]Denegación de servicio	1,00	1,0	0,0	0,0	0,0	0,0	1,0	Bajo
[B][S] Red Lan Operativa Voz y Datos	Riesgo Total		12,8	3,3	0,0	3,0	0,0	12,8	Catástrofe
	[I.8] Fallo de servicios de comunicaciones	1,00	5,0	0,0	0,0	0,0	0,0	5,0	Crítico
	[E.2]Errores del administrador del sistema\de la seguridad	1,00	2,0	2,0	0,0	0,0	0,0	2,0	Medio
	[E.9]Errores de [re-]encaminamiento	1,00	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[E.10]Errores de secuencia	1,00	0,0	1,0	0,0	0,0	0,0	1,0	Bajo
	[E.15]Alteración de información	1,00	0,0	0,1	0,0	0,0	0,0	0,1	Despreciable
	[E.19]Fugas de información	1,00	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[E.24]Caída del sistema por agotamiento de recursos	1,00	5,0	0,0	0,0	0,0	0,0	5,0	Crítico
	[A.5]Suplantación de identidad	1,00	0,0	1,0	0,0	3,0	0,0	3,0	Alto
	[A.7]Uso no previsto	10,00	10,0	10,0	0,0	0,0	0,0	10,0	Catástrofe
	[A.9][Re-]encaminamiento de mensajes	1,00	0,0	0,0	1,0	0,0	0,0	1,0	Bajo
	[A.10]Alteración de secuencia	1,00	0,0	1,0	0,0	0,0	0,0	1,0	Bajo
	[A.11]Acceso no autorizado	10,00	0,0	10,0	0,0	0,0	0,0	10,0	Catástrofe
	[A.12]Análisis de tráfico	1,00	0,0	0,0	0,2	3,0	0,0	3,0	Alto
	[A.14]Interceptación de información(escucha)	1,00	0,0	0,0	0,1	0,0	0,0	0,1	Despreciable
	[A.15]Modificación de la información	1,00	0,0	1,0	0,0	0,0	0,0	1,0	Bajo
	[A.18]Destrucción de la información	1,00	5,0	0,0	0,0	0,0	0,0	5,0	Crítico
	[A.24]Denegación de servicio	10,00	50,0	0,0	0,0	0,0	0,0	50,0	Catástrofe
[B][S] Servicio de gestión de marcación telefónica	Riesgo Total		11,2	17,2	8,1	0,0	0,0	17,2	Catástrofe
	[I.5]Avería de origen físico o lógico	1,00	5,0	0,0	0,0	0,0	0,0	5,0	Crítico
	[E.8]Difusión de software Dañino	1,00	1,0	1,0	0,9	0,0	0,0	1,0	Bajo
	[E.20]Vulnerabilidades de los programas	10,00	1,0	20,0	18,0	0,0	0,0	20,0	Catástrofe

Nom	Amenaza	Frec	D	I	C	A	T	Riesgo	Valoración
	[E.21]Errores de mantenimiento\actualización de SW	10,00	50,0	50,0	0,0	0,0	0,0	50,0	Catástrofe
	[A.8]Difusión de software dañino	1,00	5,0	5,0	4,5	0,0	0,0	5,0	Crítico
	[A.22]Manipulación de programas	1,00	5,0	10,0	9,0	0,0	0,0	10,0	Catástrofe
[B][IS][D] Base de datos operativa	Riesgo Total		0,0	3,9	4,8	0,3	0,0	4,8	Muy Alto
	[E.3] Errores de monitorización (log)	10,00	0,0	10,0	0,0	0,0	0,0	10,0	Catástrofe
	[E.15]Alteración de información	1,00	0,0	5,0	0,0	0,0	0,0	5,0	Crítico
	[E.18]Destrucción de la información	1,00	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[E.19]Fugas de información	1,00	0,0	0,0	9,0	0,0	0,0	9,0	Catástrofe
	[A.3]Manipulación de los registros de actividad (log)	1,00	0,0	3,0	0,0	0,0	0,0	3,0	Alto
	[A.5]Suplantación de identidad	0,10	0,0	0,1	0,9	0,3	0,0	0,9	Despreciable
	[A.6]Abuso de privilegios de acceso	0,10	0,0	0,1	0,5	0,0	0,0	0,5	Despreciable
	[A.11]Acceso no autorizado	1,00	0,0	5,0	9,0	0,0	0,0	9,0	Catástrofe
[A][P] Personal operativo	Riesgo Total		8,5	3,2	18,9	0,0	0,0	18,9	Catástrofe
	[E.15]Alteración de información	10,00	0,0	7,0	0,0	0,0	0,0	7,0	Extremadamente Crítico
	[E.18]Destrucción de la información	1,00	3,5	0,0	0,0	0,0	0,0	3,5	Alto
	[E.19]Fugas de información	1,00	0,0	0,0	2,1	0,0	0,0	2,1	Medio
	[E.28]Indisponibilidad del personal	10,00	21,0	0,0	0,0	0,0	0,0	21,0	Catástrofe
	[A.15]Modificación de la información	1,00	0,0	3,5	0,0	0,0	0,0	3,5	Alto
	[A.18]Destrucción de la información	1,00	3,5	0,0	0,0	0,0	0,0	3,5	Alto
	[A.19]Revelación de información	10,00	0,0	0,0	35,0	0,0	0,0	35,0	Catástrofe
	[A.28]Indisponibilidad del personal	10,00	21,0	0,0	0,0	0,0	0,0	21,0	Catástrofe
	[A.29]Extorsión	1,00	1,4	1,4	3,5	0,0	0,0	3,5	Alto
	[A.20]Ingeniería Social	10,00	0,7	0,7	35,0	0,0	0,0	35,0	Catástrofe
[A][P] Personal administrativo RRHH\Finanzas\Gerencia	Riesgo Total		0,9	2,6	11,9	0,0	0,0	11,9	Catástrofe
	[E.15]Alteración de información	1,00	0,0	0,7	0,0	0,0	0,0	0,7	Despreciable
	[E.18]Destrucción de la información	1,00	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[E.19]Fugas de información	1,00	0,0	0,0	2,1	0,0	0,0	2,1	Medio
	[E.28]Indisponibilidad del personal	1,00	1,4	0,0	0,0	0,0	0,0	1,4	Bajo
	[A.15]Modificación de la información	1,00	0,0	7,0	0,0	0,0	0,0	7,0	Extremadamente Crítico
	[A.18]Destrucción de la información	1,00	0,7	0,0	0,0	0,0	0,0	0,7	Despreciable
	[A.19]Revelación de información	10,00	0,0	0,0	35,0	0,0	0,0	35,0	Catástrofe
	[A.28]Indisponibilidad del personal	1,00	1,4	0,0	0,0	0,0	0,0	1,4	Bajo
	[A.29]Extorsión	1,00	1,4	2,1	3,5	0,0	0,0	3,5	Alto
	[A.20]Ingeniería Social	1,00	0,7	0,7	7,0	0,0	0,0	7,0	Extremadamente Crítico

Nom	Amenaza	Frec	D	I	C	A	T	Riesgo	Valoración
[A][P] Personal estructura operativa	Riesgo Total		1,4	1,6	5,1	0,0	0,0	5,1	Crítico
	[E.15]Alteración de información	1,00	0,0	0,7	0,0	0,0	0,0	0,7	Despreciable
	[E.18]Destrucción de la información	1,00	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[E.19]Fugas de información	1,00	0,0	0,0	4,9	0,0	0,0	4,9	Muy Alto
	[E.28]Indisponibilidad del personal	1,00	2,1	0,0	0,0	0,0	0,0	2,1	Medio
	[A.15]Modificación de la información	1,00	0,0	3,5	0,0	0,0	0,0	3,5	Alto
	[A.18]Destrucción de la información	1,00	0,7	0,0	0,0	0,0	0,0	0,7	Despreciable
	[A.19]Revelación de información	10,00	0,0	0,0	4,9	0,0	0,0	4,9	Muy Alto
	[A.28]Indisponibilidad del personal	1,00	3,5	0,0	0,0	0,0	0,0	3,5	Alto
	[A.29]Extorsión	1,00	1,4	1,4	3,5	0,0	0,0	3,5	Alto
	[A.20]Ingeniería Social	10,00	0,7	0,7	7,0	0,0	0,0	7,0	Extremadamente Crítico
[A][L] Edificio General	Riesgo Total		3,1					3,1	Alto
	[N.1]Fuego	0,01	0,1					0,1	Despreciable
	[N.2]Daños por agua	1,00	7,2					7,2	Extremadamente Crítico
	[N.*]Desastres naturales	0,10	0,9					0,9	Despreciable
	[I.1]Fuego	0,01	0,1					0,1	Despreciable
	[I.2]Daños por agua	1,00	7,2					7,2	Extremadamente Crítico
	[I.*]Desastres industriales	0,10	0,7					0,7	Despreciable
	[I.3]Contaminación medioambiental	10,00	9,0					9,0	Catástrofe
	[I.4]Contaminación electromagnética	10,00	9,0					9,0	Catástrofe
	[A.6]Abuso de privilegios de acceso	1,00	0,9					0,9	Despreciable
	[A.7]Uso no previsto	1,00	0,9					0,9	Despreciable
	[A.26]Ataque destructivo	0,10	0,9					0,9	Despreciable
	[A.27]Ocupación enemiga	0,01	0,1					0,1	Despreciable
[A][L] Centro de datos	Riesgo Total		5,3					5,3	Crítico
	[N.1]Fuego	0,01	0,1					0,1	Despreciable
	[N.2]Daños por agua	0,01	0,1					0,1	Despreciable
	[N.*]Desastres naturales	0,10	1,0					1,0	Bajo
	[I.1]Fuego	0,01	0,1					0,1	Despreciable
	[I.2]Daños por agua	0,01	0,1					0,1	Despreciable
	[I.*]Desastres industriales	0,10	1,0					1,0	Bajo
	[I.3]Contaminación medioambiental	10,00	10,0					10,0	Catástrofe
	[I.4]Contaminación electromagnética	10,00	40,0					40,0	Catástrofe
	[A.6]Abuso de privilegios de acceso	1,00	10,0					10,0	Catástrofe
	[A.7]Uso no previsto	1,00	1,0					1,0	Bajo
	[A.26]Ataque destructivo	0,01	0,1					0,1	Despreciable
	[A.27]Ocupación enemiga	0,01	0,1					0,1	Despreciable

Nom	Amenaza	Frec	D	I	C	A	T	Riesgo	Valoración
[A][L] Locaciones operativas y administrativas	Riesgo Total		4,1					4,1	Muy Alto
	[N.1]Fuego	0,01	0,1					0,1	Despreciable
	[N.2]Daños por agua	1,00	7,2					7,2	Extremadamente Crítico
	[N.*]Desastres naturales	0,10	0,9					0,9	Despreciable
	[I.1]Fuego	0,01	0,1					0,1	Despreciable
	[I.2]Daños por agua	1,00	7,2					7,2	Extremadamente Crítico
	[I.*]Desastres industriales	1,00	9,0					9,0	Catástrofe
	[I.3]Contaminación medioambiental	1,00	0,9					0,9	Despreciable
	[I.4]Contaminación electromagnética	1,00	0,9					0,9	Despreciable
	[A.6]Abuso de privilegios de acceso	10,00	18,0					18,0	Catástrofe
	[A.7]Uso no previsto	1,00	4,5					4,5	Muy Alto
	[A.26]Ataque destructivo	0,01	0,1					0,1	Despreciable
	[A.27]Ocupación enemiga	0,01	0,1					0,1	Despreciable
[A][SS] Servicios generales mantenimiento	Riesgo Total		0,4					0,4	Despreciable
	[E.15]Alteración de información	1,00	0,0					0,0	Despreciable
	[E.18]Destrucción de la información	1,00	0,4					0,4	Despreciable
	[E.19]Fugas de información	1,00	0,0					0,0	Despreciable
	[A.15]Modificación de la información	1,00	0,0					0,0	Despreciable
	[A.18]Destrucción de la información	1,00	0,4					0,4	Despreciable
	[A.19]Revelación de información	1,00	0,0					0,0	Despreciable
	[A.28]Indisponibilidad del personal	1,00	0,4					0,4	Despreciable
	[A.29]Extorsión	1,00	0,4					0,4	Despreciable
	[A.30]Ingeniería Social	1,00	0,4					0,4	Despreciable
[A][SS] Servicio de página web	Riesgo Total		2,6	1,2	0,0	0,0	1,0	2,6	Medio
	[I.9]Interrupción de otros servicios o suministros esenciales	1,00	2,5	0,0	0,0	0,0	0,0	2,5	Medio
	[E.15]Alteración de información	1,00	0,0	0,5	0,0	0,0	0,0	0,5	Despreciable
	[E.18]Destrucción de la información	1,00	0,5	0,0	0,0	0,0	0,0	0,5	Despreciable
	[E.19]Fugas de información	1,00	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[A.5]Suplantación de identidad	0,10	0,0	0,5	0,0	0,0	0,0	0,5	Despreciable
	[A.13]Repudio (negación de actuaciones)	1,00	0,0	0,0	0,0	0,0	1,0	1,0	Bajo
	[A.15]Modificación de la información	1,00	0,0	2,5	0,0	0,0	0,0	2,5	Medio
	[A.18]Destrucción de la información	1,00	2,5	0,0	0,0	0,0	0,0	2,5	Medio
	[A.19]Revelación de información	1,00	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[A.24]Denegación de servicio	1,00	5,0	0,0	0,0	0,0	0,0	5,0	Crítico
[A][SS] Servicio de correo electrónico	Riesgo Total		2,0	1,4	1,4	0,5	0,0	2,0	Medio
	[I.9]Interrupción de otros servicios o suministros esenciales	1,00	2,5	0,0	0,0	0,0	0,0	2,5	Medio
	[E.15]Alteración de información	1,00	0,0	0,6	0,0	0,0	0,0	0,6	Despreciable

Nom	Amenaza	Frec	D	I	C	A	T	Riesgo	Valoración
	[E.18]Destrucción de la información	1,00	0,5	0,0	0,0	0,0	0,0	0,5	Despreciable
	[E.19]Fugas de información	1,00	0,0	0,0	0,6	0,0	0,0	0,6	Despreciable
	[A.5]Suplantación de identidad	0,10	0,0	0,6	0,6	0,5	0,0	0,6	Despreciable
	[A.13]Repudio (negación de actuaciones)	1,00	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[A.15]Modificación de la información	1,00	0,0	3,0	0,0	0,0	0,0	3,0	Alto
	[A.18]Destrucción de la información	1,00	2,5	0,0	0,0	0,0	0,0	2,5	Medio
	[A.19]Revelación de información	1,00	0,0	0,0	3,0	0,0	0,0	3,0	Alto
	[A.24]Denegación de servicio	1,00	2,5	0,0	0,0	0,0	0,0	2,5	Medio
[A][SS] Servicio de líneas móviles	Riesgo Total		1,4	1,2	5,4	0,0	0,0	5,4	Crítico
	[I.8]Fallo de servicios de comunicaciones	0,10	0,2	0,0	0,0	0,0	0,0	0,2	Despreciable
	[E.2]Errores del administrador del sistema\de la seguridad	0,10	0,1	0,1	0,1	0,0	0,0	0,1	Despreciable
	[E.9]Errores de [re-]encaminamiento	0,10	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[E.10]Errores de secuencia	0,10	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[E.15]Alteración de información	0,10	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[E.19]Fugas de información	10,00	0,0	0,0	15,0	0,0	0,0	15,0	Catástrofe
	[E.24]Caída del sistema por agotamiento de recursos	0,10	0,2	0,0	0,0	0,0	0,0	0,2	Despreciable
	[A.5]Suplantación de identidad	10,00	0,0	3,0	15,0	0,0	0,0	15,0	Catástrofe
	[A.7]Uso no previsto	10,00	4,0	3,0	3,0	0,0	0,0	4,0	Muy Alto
	[A.9][Re-]encaminamiento de mensajes	1,00	0,0	0,0	0,3	0,0	0,0	0,3	Despreciable
	[A.10]Alteración de secuencia	1,00	0,0	0,3	0,0	0,0	0,0	0,3	Despreciable
	[A.11]Acceso no autorizado	10,00	0,0	3,0	15,0	0,0	0,0	15,0	Catástrofe
	[A.12]Análisis de tráfico	1,00	0,0	0,0	0,1	0,0	0,0	0,1	Despreciable
	[A.14]Interceptación de información(escucha)	0,10	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[A.15]Modificación de la información	0,10	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[A.18]Destrucción de la información	1,00	2,0	0,0	0,0	0,0	0,0	2,0	Medio
	[A.24]Denegación de servicio	1,00	2,0	0,0	0,0	0,0	0,0	2,0	Medio
[A][SW] Software ofimático	Riesgo Total		4,7	4,3	0,0	0,0	0,0	4,7	Muy Alto
	[I.5]Avería de origen físico o lógico	1,00	2,0	0,0	0,0	0,0	0,0	2,0	Medio
	[E.8]Difusión de software Dañino	10,00	4,0	3,0	0,0	0,0	0,0	4,0	Muy Alto
	[E.20]Vulnerabilidades de los programas	1,00	0,0	0,6	0,0	0,0	0,0	0,6	Despreciable
	[E.21]Errores de mantenimiento\actualización de SW	1,00	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[A.8]Difusión de software dañino	10,00	20,0	15,0	0,0	0,0	0,0	20,0	Catástrofe
	[A.22]Manipulación de programas	1,00	2,0	3,0	0,0	0,0	0,0	3,0	Alto

Nom	Amenaza	Frec	D	I	C	A	T	Riesgo	Valoración
[A][SW] Software antivirus	Riesgo Total		2,6	1,4	0,0	0,0	0,0	2,6	Medio
	[I.5]Avería de origen físico o lógico	1,00	3,5	0,0	0,0	0,0	0,0	3,5	Alto
	[E.8]Difusión de software Dañino	1,00	0,7	0,3	0,0	0,0	0,0	0,7	Despreciable
	[E.20]Vulnerabilidades de los programas	1,00	0,1	0,6	0,0	0,0	0,0	0,6	Despreciable
	[E.21]Errores de mantenimiento\actualización de SW	10,00	0,7	0,3	0,0	0,0	0,0	0,7	Despreciable
	[A.8]Difusión de software dañino	1,00	7,0	3,0	0,0	0,0	0,0	7,0	Extremadamente Crítico
	[A.22]Manipulación de programas	1,00	3,5	3,0	0,0	0,0	0,0	3,5	Alto
[A][SW] Software administrativo-contabilidad-RRHH	Riesgo Total		10,5	10,1	14,4	0,0	0,0	14,4	Catástrofe
	[I.5]Avería de origen físico o lógico	1,00	4,5	0,0	0,0	0,0	0,0	4,5	Muy Alto
	[E.8]Difusión de software Dañino	10,00	9,0	7,0	8,0	0,0	0,0	9,0	Catástrofe
	[E.20]Vulnerabilidades de los programas	1,00	0,1	1,4	1,6	0,0	0,0	1,6	Bajo
	[E.21]Errores de mantenimiento\actualización de SW	1,00	0,1	0,1	0,0	0,0	0,0	0,1	Despreciable
	[A.8]Difusión de software dañino	10,00	45,0	35,0	40,0	0,0	0,0	45,0	Catástrofe
	[A.22]Manipulación de programas	1,00	4,5	7,0	8,0	0,0	0,0	8,0	Desastre
[A][HW] Equipos de escritorio - laptops	Riesgo Total		12,2	10,1	14,7	0,0	0,0	14,7	Catástrofe
	[N.1]Fuego	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[N.2]Daños por agua	1,00	2,7	0,0	0,0	0,0	0,0	2,7	Medio
	[N.*]Desastres naturales	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[I.1]Fuego	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[I.2]Daños por agua	1,00	2,7	0,0	0,0	0,0	0,0	2,7	Medio
	[I.*]Desastres industriales	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[I.3]Contaminación medioambiental	0,10	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[I.4]Contaminación electromagnética	1,00	0,9	0,0	0,0	0,0	0,0	0,9	Despreciable
	[I.5]Avería de origen físico o lógico	10,00	45,0	0,0	0,0	0,0	0,0	45,0	Catástrofe
	[I.6]Corte del suministro eléctrico	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[I.7]Condiciones Inadecuadas de temperatura o humedad	1,00	4,5	0,0	0,0	0,0	0,0	4,5	Muy Alto
	[I.11]Emanaciones electromagnéticas	1,00	0,0	0,0	0,1	0,0	0,0	0,1	Despreciable
	[E.8]Difusión de software Dañino	10,00	27,0	15,0	21,0	0,0	0,0	27,0	Catástrofe
	[E.20]Vulnerabilidades de los programas	10,00	27,0	15,0	21,0	0,0	0,0	27,0	Catástrofe
	[E.21]Errores de mantenimiento\actualización de SW	10,00	27,0	15,0	0,0	0,0	0,0	27,0	Catástrofe
	[E.23]Errores de mantenimiento\actualización de HW	10,00	27,0	0,0	0,0	0,0	0,0	27,0	Catástrofe
	[E.24]Caída del sistema por agotamiento de recursos	10,00	45,0	0,0	0,0	0,0	0,0	45,0	Catástrofe
	[E.25]Pérdida de equipos	0,01	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[A.7]Uso no previsto	10,00	9,0	0,5	7,0	0,0	0,0	9,0	Catástrofe

Nom	Amenaza	Frec	D	I	C	A	T	Riesgo	Valoración
	[A.8]Difusión de software dañino	10,00	27,0	15,0	21,0	0,0	0,0	27,0	Catástrofe
	[A.11]Acceso no autorizado	10,00	9,0	5,0	35,0	0,0	0,0	35,0	Catástrofe
	[A.22]Manipulación de programas	1,00	4,5	5,0	7,0	0,0	0,0	7,0	Extremadamente Crítico
	[A.23]Manipulación del hardware	10,00	45,0	0,0	35,0	0,0	0,0	45,0	Catástrofe
	[A.24]Denegación de servicio	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[A.25]Robo de equipos	0,01	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[A.26]Ataque destructivo	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
[A][HW] Servidores	Riesgo Total		3,1	3,6	2,8	0,7	0,7	3,6	Alto
	[N.1]Fuego	0,10	1,0	0,0	0,0	0,0	0,0	1,0	Bajo
	[N.2]Daños por agua	0,10	1,0	0,0	0,0	0,0	0,0	1,0	Bajo
	[N.*]Desastres naturales	0,10	1,0	0,0	0,0	0,0	0,0	1,0	Bajo
	[I.1]Fuego	0,10	1,0	0,0	0,0	0,0	0,0	1,0	Bajo
	[I.2]Daños por agua	0,10	1,0	0,0	0,0	0,0	0,0	1,0	Bajo
	[I.*]Desastres industriales	0,10	1,0	0,0	0,0	0,0	0,0	1,0	Bajo
	[I.3]Contaminación medioambiental	0,10	1,0	0,0	0,0	0,0	0,0	1,0	Bajo
	[I.4]Contaminación electromagnética	0,10	1,0	0,0	0,0	0,0	0,0	1,0	Bajo
	[I.5]Avería de origen físico o lógico	1,00	10,0	0,0	0,0	0,0	0,0	10,0	Catástrofe
	[I.6]Corte del suministro eléctrico	0,10	1,0	0,0	0,0	0,0	0,0	1,0	Bajo
	[I.7]Condiciones Inadecuadas de temperatura o humedad	0,10	1,0	0,0	0,0	0,0	0,0	1,0	Bajo
	[I.10]Degradación de los soportes de almacenamiento	0,10	1,0	0,0	0,0	0,0	0,0	1,0	Bajo
	[I.11]Emanaciones electromagnéticas	0,10	0,0	0,0	0,5	0,0	0,0	0,5	Despreciable
	[E.1]Errores de los usuarios	0,01	0,1	0,1	0,1	0,0	0,0	0,1	Despreciable
	[E.2]Errores del admin del sistema\de la seguridad	1,00	10,0	9,0	9,0	0,0	0,0	10,0	Catástrofe
	[E.3] Errores de monitorización (log)	1,00	0,0	4,5	0,0	0,0	0,0	4,5	Muy Alto
	[E.4]Errores de configuración	0,10	0,0	0,9	0,0	0,0	0,0	0,9	Despreciable
	[E.8]Difusión de software Dañino	1,00	10,0	9,0	9,0	0,0	0,0	10,0	Catástrofe
	[E.15]Alteración de información	0,01	0,0	0,1	0,0	0,0	0,0	0,1	Despreciable
	[E.18]Destrucción de la información	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[E.19]Fugas de información	0,10	0,0	0,0	0,9	0,0	0,0	0,9	Despreciable
	[E.20]Vulnerabilidades de los programas	1,00	5,0	4,5	4,5	0,0	0,0	5,0	Crítico
	[E.21]Errores de mantenimiento\actualización de SW	1,00	10,0	4,5	0,0	0,0	0,0	10,0	Catástrofe
	[E.23]Errores de mantenimiento\actualización de HW	0,10	1,0	0,0	0,0	0,0	0,0	1,0	Bajo
	[E.24]Caída del sistema por agotamiento de recursos	1,00	10,0	0,0	0,0	0,0	0,0	10,0	Catástrofe
	[E.25]Pérdida de equipos	0,01	0,1	0,0	0,1	0,0	0,0	0,1	Despreciable
	[A.3]Manipulación de los registros de actividad (log)	0,10	0,0	0,5	0,0	0,0	0,0	0,5	Despreciable

Nom	Amenaza	Frec	D	I	C	A	T	Riesgo	Valoración
	[A.4]Manipulación de los ficheros de configuración	1,00	10,0	9,0	9,0	0,0	0,0	10,0	Catástrofe
	[A.5]Suplantación de identidad	0,10	0,0	0,5	0,9	1,0	0,0	1,0	Bajo
	[A.6]Abuso de privilegios de acceso	0,10	0,0	0,3	0,9	1,0	0,0	1,0	Bajo
	[A.7]Uso no previsto	0,01	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[A.8]Difusión de software dañino	1,00	10,0	9,0	9,0	0,0	0,0	10,0	Catástrofe
	[A.11]Acceso no autorizado	0,01	0,0	0,0	0,0	0,1	0,0	0,1	Despreciable
	[A.13]Repudio (negación de actuaciones)	0,10	0,0	0,0	0,0	0,0	0,7	0,7	Despreciable
	[A.15]Modificación de la información	1,00	0,0	9,0	0,0	0,0	0,0	9,0	Catástrofe
	[A.18]Destrucción de la información	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[A.22]Manipulación de programas	0,10	1,0	0,9	0,9	0,0	0,0	1,0	Bajo
	[A.23]Manipulación del hardware	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[A.24]Denegación de servicio	1,00	10,0	0,0	0,0	0,0	0,0	10,0	Catástrofe
	[A.25]Robo de equipos	0,01	0,1	0,0	0,1	0,0	0,0	0,1	Despreciable
	[A.26]Ataque destructivo	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
[A][HW] Equipos de telefonía móvil	Riesgo Total		5,6	4,7	5,6	0,0	0,0	5,6	Crítico
	[N.1]Fuego	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[N.2]Daños por agua	1,00	5,0	0,0	0,0	0,0	0,0	5,0	Crítico
	[N.*]Desastres naturales	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[I.1]Fuego	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[I.2]Daños por agua	1,00	5,0	0,0	0,0	0,0	0,0	5,0	Crítico
	[I.*]Desastres industriales	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[I.3]Contaminación medioambiental	1,00	0,5	0,0	0,0	0,0	0,0	0,5	Despreciable
	[I.4]Contaminación electromagnética	1,00	0,5	0,0	0,0	0,0	0,0	0,5	Despreciable
	[I.5]Avería de origen físico o lógico	0,01	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[I.6]Corte del suministro eléctrico	0,01	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[I.7]Condiciones Inadecuadas de temperatura o humedad	10,00	15,0	0,0	0,0	0,0	0,0	15,0	Catástrofe
	[I.11]Emanaciones electromagnéticas	1,00	0,0	0,0	0,1	0,0	0,0	0,1	Despreciable
	[E.8]Difusión de software Dañino	10,00	15,0	8,0	10,0	0,0	0,0	15,0	Catástrofe
	[E.20]Vulnerabilidades de los programas	0,10	0,2	0,1	0,1	0,0	0,0	0,2	Despreciable
	[E.21]Errores de mantenimiento\actualización de SW	1,00	1,5	0,8	0,0	0,0	0,0	1,5	Bajo
	[E.23]Errores de mantenimiento\actualización de HW	1,00	1,5	0,0	0,0	0,0	0,0	1,5	Bajo
	[E.24]Caída del sistema por agotamiento de recursos	0,10	0,5	0,0	0,0	0,0	0,0	0,5	Despreciable
	[E.25]Pérdida de equipos	1,00	5,0	0,0	1,0	0,0	0,0	5,0	Crítico
	[A.7]Uso no previsto	10,00	5,0	4,0	5,0	0,0	0,0	5,0	Crítico
	[A.8]Difusión de software dañino	10,00	15,0	8,0	10,0	0,0	0,0	15,0	Catástrofe
	[A.11]Acceso no autorizado	10,00	5,0	4,0	10,0	0,0	0,0	10,0	Catástrofe

Nom	Amenaza	Frec	D	I	C	A	T	Riesgo	Valoración
	[A.22]Manipulación de programas	10,00	15,0	8,0	10,0	0,0	0,0	15,0	Catástrofe
	[A.23]Manipulación del hardware	0,01	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[A.24]Denegación de servicio	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[A.25]Robo de equipos	10,00	50,0	0,0	10,0	0,0	0,0	50,0	Catástrofe
	[A.26]Ataque destructivo	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
[A][AUX] Sistema de alimentación ininterrumpido	Riesgo Total		2,3	0,0	0,0	0,0	0,0	2,3	Medio
	[N.1]Fuego	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[N.2]Daños por agua	1,00	10,0	0,0	0,0	0,0	0,0	10,0	Catástrofe
	[N.*]Desastres naturales	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[I.1]Fuego	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[I.2]Daños por agua	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[I.*]Desastres industriales	0,10	1,0	0,0	0,0	0,0	0,0	1,0	Bajo
	[I.3]Contaminación medioambiental	0,10	0,5	0,0	0,0	0,0	0,0	0,5	Despreciable
	[E.23]Errores de mantenimiento\actualización de HW	1,00	5,0	0,0	0,0	0,0	0,0	5,0	Crítico
	[A.7]Uso no previsto	1,00	5,0	0,0	0,0	0,0	0,0	5,0	Crítico
	[A.23]Manipulación del hardware	1,00	5,0	0,0	0,0	0,0	0,0	5,0	Crítico
	[A.25]Robo de equipos	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[A.26]Ataque destructivo	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
[A][AUX] Generador eléctrico de respaldo	Riesgo Total		1,3	0,0	0,0	0,0	0,0	1,3	Bajo
	[N.1]Fuego	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[N.2]Daños por agua	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[N.*]Desastres naturales	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[I.1]Fuego	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[I.2]Daños por agua	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[I.*]Desastres industriales	0,10	0,9	0,0	0,0	0,0	0,0	0,9	Despreciable
	[I.3]Contaminación medioambiental	1,00	4,5	0,0	0,0	0,0	0,0	4,5	Muy Alto
	[E.23]Errores de mantenimiento\actualización de HW	1,00	4,5	0,0	0,0	0,0	0,0	4,5	Muy Alto
	[A.7]Uso no previsto	0,01	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[A.23]Manipulación del hardware	1,00	4,5	0,0	0,0	0,0	0,0	4,5	Muy Alto
	[A.25]Robo de equipos	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[A.26]Ataque destructivo	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
[A][AUX] Cableado eléctrico Centro	Riesgo Total		1,7	0,0	0,0	0,0	0,0	1,7	Bajo
	[N.1]Fuego	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[N.2]Daños por agua	0,01	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[N.*]Desastres naturales	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[I.1]Fuego	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[I.2]Daños por agua	0,01	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[I.*]Desastres industriales	1,00	9,0	0,0	0,0	0,0	0,0	9,0	Catástrofe

Nom	Amenaza	Frec	D	I	C	A	T	Riesgo	Valoración
	[I.3]Contaminación medioambiental	1,00	2,7	0,0	0,0	0,0	0,0	2,7	Medio
	[I.4]Contaminación electromagnética	1,00	2,7	0,0	0,0	0,0	0,0	2,7	Medio
	[I.11]Emanaciones electromagnéticas	1,00	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[E.23]Errores de mantenimiento\actualización de HW	1,00	2,7	0,0	0,0	0,0	0,0	2,7	Medio
	[A.7]Uso no previsto	0,01	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[A.11]Acceso no autorizado	0,01	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[A.23]Manipulación del hardware	1,00	4,5	0,0	0,0	0,0	0,0	4,5	Muy Alto
	[A.25]Robo de equipos	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[A.26]Ataque destructivo	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
[A][AUX] Cableado fibra óptica	Riesgo Total		2,4	0,0	0,0	0,0	0,0	2,4	Medio
	[N.1]Fuego	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[N.2]Daños por agua	0,01	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[N.*]Desastres naturales	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[I.1]Fuego	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[I.2]Daños por agua	0,01	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[I.*]Desastres industriales	0,10	0,9	0,0	0,0	0,0	0,0	0,9	Despreciable
	[I.3]Contaminación medioambiental	1,00	4,5	0,0	0,0	0,0	0,0	4,5	Muy Alto
	[E.23]Errores de mantenimiento\actualización de HW	1,00	9,0	0,0	0,0	0,0	0,0	9,0	Catástrofe
	[A.7]Uso no previsto	1,00	4,5	0,0	0,0	0,0	0,0	4,5	Muy Alto
	[A.23]Manipulación del hardware	1,00	9,0	0,0	0,0	0,0	0,0	9,0	Catástrofe
	[A.25]Robo de equipos	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[A.26]Ataque destructivo	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
[A][AUX] Impresoras Operativas y Administrativas	Riesgo Total		0,3	0,0	0,0	0,0	0,0	0,3	Despreciable
	[N.1]Fuego	0,01	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[N.2]Daños por agua	0,01	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[N.*]Desastres naturales	0,01	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[I.1]Fuego	0,01	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[I.2]Daños por agua	0,01	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[I.*]Desastres industriales	0,01	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[I.3]Contaminación medioambiental	0,01	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[I.4]Contaminación electromagnética	0,01	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[I.5]Avería de origen físico o lógico	1	2,0	0,0	0,0	0,0	0,0	2,0	Medio
	[I.6]Corte del suministro eléctrico	0,1	0,2	0,0	0,0	0,0	0,0	0,2	Despreciable
	[I.7]Condiciones Inadecuadas de temperatura o humedad	0,1	0,2	0,0	0,0	0,0	0,0	0,2	Despreciable
	[I.11]Emanaciones electromagnéticas	0,1	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[E.23]Errores de mantenimiento\actualización de HW	1	1,0	0,0	0,0	0,0	0,0	1,0	Bajo
	[E.24]Caída del sistema por agotamiento de recursos	0,1	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable

Nom	Amenaza	Frec	D	I	C	A	T	Riesgo	Valoración
	[E.25]Pérdida de equipos	0,01	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[A.11]Acceso no autorizado	1	0,2	0,0	0,0	0,0	0,0	0,2	Despreciable
	[A.23]Manipulación del hardware	1	2,0	0,0	0,0	0,0	0,0	2,0	Medio
	[A.24]Denegación de servicio	0,1	0,2	0,0	0,0	0,0	0,0	0,2	Despreciable
	[A.25]Robo de equipos	0,01	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[A.26]Ataque destructivo	0,01	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
[A][AUX] Servicio Backups	Riesgo Total		1,9	12,6	1,6	3,6	9,0	12,6	Catástrofe
	[N.1]Fuego	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[N.2]Daños por agua	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[N.*]Desastres naturales	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[I.1]Fuego	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[I.2]Daños por agua	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[I.*]Desastres industriales	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[I.3]Contaminación medioambiental	1,00	4,5	0,0	0,0	0,0	0,0	4,5	Muy Alto
	[I.4]Contaminación electromagnética	1,00	9,0	0,0	0,0	0,0	0,0	9,0	Catástrofe
	[I.5]Avería de origen físico o lógico	1,00	9,0	0,0	0,0	0,0	0,0	9,0	Catástrofe
	[I.6]Corte del suministro eléctrico	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[I.7]Condiciones Inadecuadas de temperatura o humedad	1,00	9,0	0,0	0,0	0,0	0,0	9,0	Catástrofe
	[I.10]Degradación de los soportes de almacenamiento	0,10	0,9	0,0	0,0	0,0	0,0	0,9	Despreciable
	[I.11]Emanaciones electromagnéticas	1,00	0,0	0,0	0,1	0,0	0,0	0,1	Despreciable
	[E.1]Errores de los usuarios	1,00	4,5	4,5	4,5	0,0	0,0	4,5	Muy Alto
	[E.2]Errores del administrador del sistema\de la seguridad	0,10	0,5	0,5	0,5	0,0	0,0	0,5	Despreciable
	[E.15]Alteración de información	0,10	0,0	0,5	0,0	0,0	0,0	0,5	Despreciable
	[E.18]Destrucción de la información	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[E.19]Fugas de información	0,10	0,0	0,0	0,9	0,0	0,0	0,9	Despreciable
	[E.23]Errores de mantenimiento\actualización de HW	0,10	0,9	0,0	0,0	0,0	0,0	0,9	Despreciable
	[E.24]Caída del sistema por agotamiento de recursos	0,10	0,9	0,0	0,0	0,0	0,0	0,9	Despreciable
	[E.25]Pérdida de equipos	0,10	0,9	0,0	0,9	0,0	0,0	0,9	Despreciable
	[A.5]Suplantación de identidad	0,10	0,0	0,5	0,5	0,9	0,0	0,9	Despreciable
	[A.6]Abuso de privilegios de acceso	0,10	0,0	0,5	0,9	0,9	0,0	0,9	Despreciable
	[A.7]Uso no previsto	0,10	0,0	0,1	0,1	0,0	0,0	0,1	Despreciable
	[A.11]Acceso no autorizado	1,00	0,0	4,5	9,0	9,0	0,0	9,0	Catástrofe
	[A.13]Repudio (negación de actuaciones)	1,00	0,0	0,0	0,0	0,0	9,0	9,0	Catástrofe
	[A.15]Modificación de la información	10,00	0,0	90,0	0,0	0,0	0,0	90,0	Catástrofe
	[A.18]Destrucción de la información	0,10	0,9	0,0	0,0	0,0	0,0	0,9	Despreciable
	[A.23]Manipulación del hardware	0,01	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable

Nom	Amenaza	Frec	D	I	C	A	T	Riesgo	Valoración
	[A.24]Denegación de servicio	1,00	4,5	0,0	0,0	0,0	0,0	4,5	Muy Alto
	[A.25]Robo de equipos	0,01	0,1	0,0	0,1	0,0	0,0	0,1	Despreciable
	[A.26]Ataque destructivo	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
[A][COM] Switches Core y Distribuidores	Riesgo Total		1,8	0,0	0,0	0,0	0,0	1,8	Bajo
	[N.1]Fuego	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[N.2]Daños por agua	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[N.*]Desastres naturales	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[I.1]Fuego	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[I.2]Daños por agua	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[I.*]Desastres industriales	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[I.3]Contaminación medioambiental	1,00	4,5	0,0	0,0	0,0	0,0	4,5	Muy Alto
	[I.4]Contaminación electromagnética	0,10	0,5	0,0	0,0	0,0	0,0	0,5	Despreciable
	[I.5]Avería de origen físico o lógico	0,10	0,9	0,0	0,0	0,0	0,0	0,9	Despreciable
	[I.6]Corte del suministro eléctrico	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[I.7]Condiciones Inadecuadas de temperatura o humedad	0,10	0,9	0,0	0,0	0,0	0,0	0,9	Despreciable
	[I.11]Emanaciones electromagnéticas	0,10	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[E.23]Errores de mantenimiento\actualización de HW	1,00	4,5	0,0	0,0	0,0	0,0	4,5	Muy Alto
	[E.24]Caída del sistema por agotamiento de recursos	1,00	4,5	0,0	0,0	0,0	0,0	4,5	Muy Alto
	[E.25]Pérdida de equipos	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[A.7]Uso no previsto	0,10	0,5	0,0	0,0	0,0	0,0	0,5	Despreciable
	[A.11]Acceso no autorizado	0,10	0,5	0,0	0,0	0,0	0,0	0,5	Despreciable
	[A.23]Manipulación del hardware	1,00	9,0	0,0	0,0	0,0	0,0	9,0	Catástrofe
	[A.24]Denegación de servicio	1,00	9,0	0,0	0,0	0,0	0,0	9,0	Catástrofe
	[A.25]Robo de equipos	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[A.26]Ataque destructivo	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
[A][COM] Firewall	Riesgo Total		3,0	0,5	0,7	0,0	0,0	3,0	Medio
	[N.1]Fuego	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[N.2]Daños por agua	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[N.*]Desastres naturales	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[I.1]Fuego	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[I.2]Daños por agua	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[I.*]Desastres industriales	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[I.3]Contaminación medioambiental	1,00	5,0	0,0	0,0	0,0	0,0	5,0	Crítico
	[I.4]Contaminación electromagnética	1,00	5,0	0,0	0,0	0,0	0,0	5,0	Crítico
	[I.5]Avería de origen físico o lógico	0,10	1,0	0,0	0,0	0,0	0,0	1,0	Bajo
	[I.6]Corte del suministro eléctrico	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[I.7]Condiciones Inadecuadas de temperatura o humedad	0,10	1,0	0,0	0,0	0,0	0,0	1,0	Bajo

Nom	Amenaza	Frec	D	I	C	A	T	Riesgo	Valoración
	[I.11]Emanaciones electromagnéticas	1,00	0,0	0,0	0,1	0,0	0,0	0,1	Despreciable
	[E.8]Difusión de software Dañino	1,00	10,0	0,9	2,1	0,0	0,0	10,0	Catástrofe
	[E.20]Vulnerabilidades de los programas	1,00	5,0	0,6	2,1	0,0	0,0	5,0	Crítico
	[E.21]Errores de mantenimiento\actualización de SW	1,00	10,0	0,6	0,0	0,0	0,0	10,0	Catástrofe
	[E.23]Errores de mantenimiento\actualización de HW	1,00	10,0	0,0	0,0	0,0	0,0	10,0	Catástrofe
	[E.24]Caída del sistema por agotamiento de recursos	1,00	10,0	0,0	0,0	0,0	0,0	10,0	Catástrofe
	[E.25]Pérdida de equipos	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[A.7]Uso no previsto	0,10	0,5	0,0	0,2	0,0	0,0	0,5	Despreciable
	[A.8]Difusión de software dañino	1,00	5,0	0,9	2,1	0,0	0,0	5,0	Crítico
	[A.11]Acceso no autorizado	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[A.22]Manipulación de programas	0,10	0,5	0,1	0,2	0,0	0,0	0,5	Despreciable
	[A.23]Manipulación del hardware	0,10	1,0	0,0	0,2	0,0	0,0	1,0	Bajo
	[A.24]Denegación de servicio	0,10	1,0	0,0	0,0	0,0	0,0	1,0	Bajo
	[A.25]Robo de equipos	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[A.26]Ataque destructivo	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
[A][COM] Canal de internet principal y backup	Riesgo Total		8,1	1,2	0,8	1,7	3,0	8,1	Desastre
	[I.8]Fallo de servicios de comunicaciones	1,00	7,0	0,0	0,0	0,0	0,0	7,0	Extremadamente Crítico
	[E.2]Errores del administrador del sistema\de la seguridad	0,10	0,4	0,4	0,1	0,0	0,0	0,4	Despreciable
	[E.9]Errores de [re-]encaminamiento	0,10	0,0	0,0	0,2	0,0	0,0	0,2	Despreciable
	[E.10]Errores de secuencia	0,10	0,0	0,4	0,0	0,0	0,0	0,4	Despreciable
	[E.15]Alteración de información	0,10	0,0	0,4	0,0	0,0	0,0	0,4	Despreciable
	[E.18]Destrucción de la información	0,01	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[E.19]Fugas de información	0,10	0,0	0,0	0,2	0,0	0,0	0,2	Despreciable
	[E.24]Caída del sistema por agotamiento de recursos	1,00	7,0	0,0	0,0	0,0	0,0	7,0	Extremadamente Crítico
	[A.5]Suplantación de identidad	0,10	0,0	0,4	0,2	0,3	0,0	0,4	Despreciable
	[A.7]Uso no previsto	10,00	35,0	7,0	3,0	0,0	0,0	35,0	Catástrofe
	[A.9][Re-]encaminamiento de mensajes	0,10	0,0	0,0	0,2	0,0	0,0	0,2	Despreciable
	[A.10]Alteración de secuencia	0,10	0,0	0,4	0,0	0,0	0,0	0,4	Despreciable
	[A.11]Acceso no autorizado	1,00	0,0	0,7	1,5	3,0	0,0	3,0	Alto
	[A.12]Análisis de tráfico	1,00	0,0	0,0	1,5	0,0	0,0	1,5	Bajo
	[A.13]Repudio (negación de actuaciones)	1,00	0,0	0,0	0,0	0,0	3,0	3,0	Alto
	[A.14]Interceptación de información(escucha)	1,00	0,0	0,0	1,5	0,0	0,0	1,5	Bajo
	[A.15]Modificación de la información	0,10	0,0	0,4	0,0	0,0	0,0	0,4	Despreciable
	[A.18]Destrucción de la información	0,01	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable

Nom	Amenaza	Frec	D	I	C	A	T	Riesgo	Valoración
	[A.19]Revelación de información	0,01	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[A.24]Denegación de servicio	1,00	7,0	0,0	0,0	0,0	0,0	7,0	Extremadamente Crítico
[A][COM] Canal de MPLS casa matriz Ppal y BCK	Riesgo Total		8,1	1,2	1,9	3,9	0,0	8,1	Desastre
	[I.8]Fallo de servicios de comunicaciones	1,00	7,0	0,0	0,0	0,0	0,0	7,0	Extremadamente Crítico
	[E.2]Errores del administrador del sistema\de la seguridad	0,10	0,4	0,4	0,2	0,0	0,0	0,4	Despreciable
	[E.9]Errores de [re-]encaminamiento	0,10	0,0	0,0	0,4	0,0	0,0	0,4	Despreciable
	[E.10]Errores de secuencia	0,10	0,0	0,4	0,0	0,0	0,0	0,4	Despreciable
	[E.15]Alteración de información	0,10	0,0	0,4	0,0	0,0	0,0	0,4	Despreciable
	[E.18]Destrucción de la información	0,01	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[E.19]Fugas de información	0,10	0,0	0,0	0,4	0,0	0,0	0,4	Despreciable
	[E.24]Caída del sistema por agotamiento de recursos	1,00	7,0	0,0	0,0	0,0	0,0	7,0	Extremadamente Crítico
	[A.5]Suplantación de identidad	0,10	0,0	0,4	0,4	0,7	0,0	0,7	Despreciable
	[A.7]Uso no previsto	10,00	35,0	7,0	7,0	0,0	0,0	35,0	Catástrofe
	[A.9][Re-]encaminamiento de mensajes	0,10	0,0	0,0	0,4	0,0	0,0	0,4	Despreciable
	[A.10]Alteración de secuencia	0,10	0,0	0,4	0,0	0,0	0,0	0,4	Despreciable
	[A.11]Acceso no autorizado	1,00	0,0	0,7	3,5	7,0	0,0	7,0	Extremadamente Crítico
	[A.12]Análisis de tráfico	1,00	0,0	0,0	3,5	0,0	0,0	3,5	Alto
	[A.13]Repudio (negación de actuaciones)	1,00	0,0	0,0	0,0	0,0	7,0	7,0	Extremadamente Crítico
	[A.14]Interceptación de información(escucha)	1,00	0,0	0,0	3,5	0,0	0,0	3,5	Alto
	[A.15]Modificación de la información	0,10	0,0	0,4	0,0	0,0	0,0	0,4	Despreciable
	[A.18]Destrucción de la información	0,01	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[A.19]Revelación de información	0,01	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[A.24]Denegación de servicio	1,00	7,0	0,0	0,0	0,0	0,0	7,0	Extremadamente Crítico
[A][COM] Cableado estructura voz y datos	Riesgo Total		3,4	0,3	0,6	3,9	0,0	3,9	Alto
	[I.8]Fallo de servicios de comunicaciones	0,10	0,9	0,0	0,0	0,0	0,0	0,9	Despreciable
	[E.2]Errores del administrador del sistema\de la seguridad	0,10	0,5	0,4	0,1	0,0	0,0	0,5	Despreciable
	[E.9]Errores de [re-]encaminamiento	0,01	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[E.10]Errores de secuencia	0,01	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[E.15]Alteración de información	0,10	0,0	0,2	0,0	0,0	0,0	0,2	Despreciable
	[E.19]Fugas de información	0,10	0,0	0,0	0,7	0,0	0,0	0,7	Despreciable
	[E.24]Caída del sistema por agotamiento de recursos	1,00	9,0	0,0	0,0	0,0	0,0	9,0	Catástrofe
	[A.5]Suplantación de identidad	0,10	0,0	0,1	0,4	0,7	0,0	0,7	Despreciable
	[A.7]Uso no previsto	1,00	0,9	0,7	0,7	0,0	0,0	0,9	Despreciable

Nom	Amenaza	Frec	D	I	C	A	T	Riesgo	Valoración
	[A.9][Re-]encaminamiento de mensajes	0,01	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[A.10]Alteración de secuencia	0,01	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[A.11]Acceso no autorizado	1,00	0,0	0,7	3,5	7,0	0,0	7,0	Extremadamente Crítico
	[A.12]Análisis de tráfico	1,00	0,0	0,0	0,1	0,0	0,0	0,1	Despreciable
	[A.14]Interceptación de información(escucha)	0,10	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[A.15]Modificación de la información	0,10	0,0	0,1	0,0	0,0	0,0	0,1	Despreciable
	[A.18]Destrucción de la información	0,01	0,0	0,0	0,0	0,0	0,0	0,0	Despreciable
	[A.24]Denegación de servicio	1,00	9,0	0,0	0,0	0,0	0,0	9,0	Catástrofe
[A][IS] Serv. Tec. Aux. Ficheros configuración	Riesgo Total		0,1	0,1	0,3	0,0	0,0	0,3	Despreciable
	[E.4]Errores de configuración	0,10	0,0	0,2	0,0	0,0	0,0	0,2	Despreciable
	[E.15]Alteración de información	0,10	0,0	0,3	0,0	0,0	0,0	0,3	Despreciable
	[E.18]Destrucción de la información	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[E.19]Fugas de información	0,10	0,0	0,0	0,3	0,0	0,0	0,3	Despreciable
	[A.4]Manipulación de los ficheros de configuración	0,10	0,2	0,2	0,3	0,0	0,0	0,3	Despreciable
	[A.5]Suplantación de identidad	0,10	0,0	0,0	0,3	0,0	0,0	0,3	Despreciable
	[A.6]Abuso de privilegios de acceso	0,10	0,0	0,0	0,3	0,0	0,0	0,3	Despreciable
	[A.11]Acceso no autorizado	0,10	0,0	0,0	0,3	0,0	0,0	0,3	Despreciable
[A][IS] Serv. Tec. Aux. Manuales y Procedimientos	Riesgo Total		0,1	0,3	2,1	0,0	0,0	2,1	Medio
	[E.4]Errores de configuración	0,10	0,0	0,2	0,0	0,0	0,0	0,2	Despreciable
	[E.15]Alteración de información	0,10	0,0	0,3	0,0	0,0	0,0	0,3	Despreciable
	[E.18]Destrucción de la información	0,01	0,1	0,0	0,0	0,0	0,0	0,1	Despreciable
	[E.19]Fugas de información	1,00	0,0	0,0	2,5	0,0	0,0	2,5	Medio
	[A.4]Manipulación de los ficheros de configuración	0,10	0,2	0,2	0,3	0,0	0,0	0,3	Despreciable
	[A.5]Suplantación de identidad	1,00	0,0	0,3	2,5	0,0	0,0	2,5	Medio
	[A.6]Abuso de privilegios de acceso	1,00	0,1	0,3	2,5	0,0	0,0	2,5	Medio
	[A.11]Acceso no autorizado	1,00	0,0	0,3	2,5	0,0	0,0	2,5	Medio
[A][IS] Servicio de servidor de archivos	Riesgo Total		3,9	8,4	3,2	0,7	0,7	8,4	Desastre
	[E.1]Errores de los usuarios	10,00	14,0	21,0	7,0	0,0	0,0	21,0	Catástrofe
	[E.2]Errores del administrador del sistema\de la seguridad	0,10	0,4	0,4	0,1	0,0	0,0	0,4	Despreciable
	[E.15]Alteración de información	1,00	0,0	3,5	0,0	0,0	0,0	3,5	Alto
	[E.18]Destrucción de la información	0,10	0,7	0,0	0,0	0,0	0,0	0,7	Despreciable
	[E.19]Fugas de información	1,00	0,0	0,0	7,0	0,0	0,0	7,0	Extremadamente Crítico
	[E.24]Caída del sistema por agotamiento de recursos	0,10	0,7	0,0	0,0	0,0	0,0	0,7	Despreciable
	[A.5]Suplantación de identidad	0,10	0,0	0,4	0,4	0,7	0,0	0,7	Despreciable
	[A.6]Abuso de privilegios de acceso	0,10	0,0	0,1	0,4	0,7	0,0	0,7	Despreciable

Nom	Amenaza	Frec	D	I	C	A	T	Riesgo	Valoración
	[A.7]Uso no previsto	10,00	14,0	7,0	7,0	0,0	0,0	14,0	Catástrofe
	[A.11]Acceso no autorizado	0,10	0,0	0,1	0,4	0,7	0,0	0,7	Despreciable
	[A.13]Repudio (negación de actuaciones)	0,10	0,0	0,0	0,0	0,0	0,7	0,7	Despreciable
	[A.15]Modificación de la información	10,00	0,0	35,0	0,0	0,0	0,0	35,0	Catástrofe
	[A.18]Destrucción de la información	0,10	0,7	0,0	0,0	0,0	0,0	0,7	Despreciable
	[A.24]Denegación de servicio	0,10	0,7	0,0	0,0	0,0	0,0	0,7	Despreciable
[A][IS] Servicio de base de datos administrativa	Riesgo Total		1,3	0,4	0,4	0,7	0,7	1,3	Bajo
	[E.1]Errores de los usuarios	1,00	0,7	1,4	0,7	0,0	0,0	1,4	Bajo
	[E.2]Errores del administrador del sistema\de la seguridad	0,10	0,7	0,2	0,1	0,0	0,0	0,7	Despreciable
	[E.15]Alteración de información	0,10	0,0	0,4	0,0	0,0	0,0	0,4	Despreciable
	[E.18]Destrucción de la información	0,10	0,7	0,0	0,0	0,0	0,0	0,7	Despreciable
	[E.19]Fugas de información	0,10	0,0	0,0	0,4	0,0	0,0	0,4	Despreciable
	[E.24]Caída del sistema por agotamiento de recursos	0,10	0,7	0,0	0,0	0,0	0,0	0,7	Despreciable
	[A.5]Suplantación de identidad	0,10	0,0	0,4	0,4	0,7	0,0	0,7	Despreciable
	[A.6]Abuso de privilegios de acceso	0,10	0,0	0,1	0,4	0,7	0,0	0,7	Despreciable
	[A.7]Uso no previsto	0,10	0,0	0,1	0,4	0,0	0,0	0,4	Despreciable
	[A.11]Acceso no autorizado	0,10	0,0	0,4	0,4	0,7	0,0	0,7	Despreciable
	[A.13]Repudio (negación de actuaciones)	0,10	0,0	0,0	0,0	0,0	0,7	0,7	Despreciable
	[A.15]Modificación de la información	0,10	0,0	0,4	0,0	0,0	0,0	0,4	Despreciable
	[A.18]Destrucción de la información	0,10	0,7	0,0	0,0	0,0	0,0	0,7	Despreciable
	[A.24]Denegación de servicio	1,00	7,0	0,0	0,0	0,0	0,0	7,0	Extremadamente Crítico

Fuente: Propia

9 PROBLEMAS DETECTADOS

Telemarketing S.A.S, si bien no tiene un SGSI implementado ni ha llevado a cabo procesos de auditoría, su propia naturaleza le ha llevado a aplicar algunas prácticas que le permiten tener un nivel de seguridad que, aunque necesita mejoras, le ha permitido preservar parcialmente la seguridad de la información.

En el análisis de amenazas se ha partido sin controles establecidos, esto con el fin de hacer un análisis completo partiendo desde cero. De acuerdo con la revisión realizada se detectan los siguientes problemas junto con los puntos en los cuales se detecta el problema.

9.1 ANÁLISIS SEGÚN EL NIVEL DE RIESGO

9.1.1 Catástrofe Dentro de este nivel se encuentran fallos de servicios como el telefónico, la red LAN de voz y datos, el servicio del marcador telefónico, personal operativo y de soporte de los procesos (Administrativo) así como el software relacionado, el hardware de usuario final (Computadores), los sistemas de respaldo de información (Backups). Varios de estos elementos tienen en común que son parte esencial de la operación del negocio (servicio telefónico, red LAN, marcador telefónico y personal operativo) o son apoyo para estas labores (considerando el sector en el que se enmarca la empresa).

La caída del servicio telefónico o de la red LAN provocará la detención de las actividades de la empresa, por lo que es importante tenerla en cuenta, aun cuando no se puede decir que son servicios que sufren muchos problemas continuos, por lo que la importancia está en prevenirlos más que en corregirlos actualmente; en este sentido es importante considerar los contratos con proveedores para establecer un nivel de disponibilidad alto así como contratos y programación de mantenimiento correctamente establecido y ejecutado, esto con el fin de evitar fallos en los servicios. Igualmente es importante considerar que los servicios de red y telefonía se les del el uso adecuado, evitando el consumo de recursos en actividades que no son propias del negocio, algo que se presenta de forma regular bien sea en llamadas no autorizadas o con duraciones más allá de lo permitido o el uso del canal de datos para visualización de contenido multimedia no contemplado en las actividades, en este sentido no se identifica además un control preciso del uso de recursos, por lo que la negación de actuaciones es un riesgo real, así como el acceso no autorizado y la revelación de información.

Por otro lado, la confidencialidad e integridad son importantes dada la información que se transmite o maneja, y esto a su vez explica el nivel dado a los sistemas de *backup* pues son parte fundamental no solo en el funcionamiento sino en los requerimientos

legales de la organización; no obstante, aún la importancia de este ítem, la gestión de copias de respaldo no es completa y los usuarios no parecen conocer correctamente su uso, no hay definidas políticas de generación y prueba de los mismos.

9.1.2 Desastre Se encuentran en este nivel el canal de internet principal y secundario y el canal de MPLS además de los servidores de archivos. Esto se explica por qué son servicios de apoyo que si bien son importantes no necesariamente impiden el funcionamiento de la organización. De hecho, los servicios de internet y MPLS están sujetos a diferentes circunstancias que los pueden afectar como caídas del servicio, cortes de líneas, fallo del canal internacional, entre otros, que se pueden mitigar mediante la contratación de múltiples proveedores o diferentes tipos de tecnología. Nuevamente los contratos con los proveedores de los servicios de comunicaciones son importantes para garantizar un nivel de disponibilidad suficientemente alto para el desarrollo normal de las actividades, y también lo es los cronogramas de mantenimiento, el control de acceso a la red (lo cual no se encuentra implementado) y evitar el uso no previsto.

El servidor de archivos igualmente se encuentra sujeto a diferentes amenazas, internas y externas, pero se pude subsanar mediante políticas y gestión de copias de respaldo. Actualmente el servidor permite el acceso mediante directorio activo, sin embargo, es importante aplicar políticas de asignación de roles más precisas para evitar entre otras cosas la modificación de archivos, o la eliminación de estos.

9.1.3 Extremadamente Crítico En este nivel no se encuentra específicamente clasificado ningún activo, no obstante, si existen amenazas particulares que deberán ser consideradas dentro de las políticas para darles el tratamiento correspondiente. Entre algunos ítems clasificados en este nivel se puede encontrar:

- Se detectan posibilidades en la alteración de la información, especialmente en lo que refiere al personal administrativo y personal operativo sobre información de la organización dado que no existe un control de versiones sobre los documentos que se manejan ni logs en los servidores de archivos.

- Las posibilidades que el personal sea víctima de ataques de tipo ingeniería social es latente, pues no se identifica un nivel de capacitación suficiente en seguridad informática o seguridad de la información, o incluso actualización en el uso de tecnología.

- Las posibilidades de daños por agua están presentes, si bien no se pueden considerar frecuentes la materialización de la amenaza es posible y el efecto en las instalaciones generales puede afectar sensiblemente la operación.

- La manipulación de programas es un riesgo latente, especialmente cuando se habla de equipos de escritorio, pues son la herramienta disponible para los agentes. Nuevamente la posibilidad de materialización de la amenaza es muy baja pero no debe ser descuidada; algunas aplicaciones requieren mejorar el control de acceso y cuidar la manipulación de la información en los diferentes repositorios.

9.1.4 Muy Crítico No hay activos ni amenazas con este nivel de riesgo.

9.1.5 Crítico El personal de estructura operativa se encuentra en este nivel de riesgo, dado que es un apoyo importante para la operación. También lo está el centro de datos que si bien es fundamental su protección hace la que probabilidad de materialización de una amenaza sea suficientemente bajo para no ser considerado en un nivel más alto. El servicio de líneas y los equipos móviles también están clasificada como crítico, especialmente por el nivel de confidencialidad, pues la posibilidad de robos y el manejo de información sensible en ellos los convierte en un punto débil de la organización.

Dentro del análisis realizado se ha identificado la posibilidad de fallos en los servicios que afectarían la normal operación, esto dado por condiciones propias de dichos servicios como latencias, caídas, entre otros; esta no es una amenaza con probabilidad alta de ocurrencia, pero es algo a considerar, al igual que una posible caída de diferentes sistemas por agotamiento de recursos (bien sea internos o externos).

Por otro lado, la información requiere ser protegida dado que no se cuentan con las condiciones adecuadas de respaldo, incluso los miembros de la organización desconocen las medidas disponibles para respaldar sus datos y están expuestos a riesgos como la eliminación o la alteración. Esto se suma también a la exposición a software dañino y vulnerabilidades de los programas, esto último potenciado por falta de mantenimiento y/o actualización de software, sin descartar además los riesgos asociados al hardware como falta de actualización y pérdida (especialmente para equipos móviles.

9.1.6 Muy alto La base de datos operativa junto con las locaciones operativas y administrativas y el software ofimático hacen parte de este nivel de riesgo. En el caso de la BD es un sistema protegido y respaldado, por lo que la probabilidad de ocurrencia lo mantiene en este nivel, mientras las locaciones operativas y administrativas no suelen estar expuestas a amenazas con niveles de degradación o frecuencias altos (nuevamente).

No obstante, en cuanto a la BD, se requiere mejorar los niveles de encriptación de la información y las políticas de gestión de usuarios y contraseñas del sistema, de tal manera que sea más controlado el acceso (respecto a lo que es actualmente). En cuanto a las locaciones operativas y administrativas, el acceso a dichas zonas puede mejorar sensiblemente para evitar el acceso no controlado a ellas y a los recursos allí contenidos.

El software ofimático es un apoyo a las operaciones, pero no impacta en el funcionamiento de la empresa, aunque si lo puede hacer el observar que no se cuenta con los licenciamientos necesarios y esto si puede impactar en cuestiones legales y la imagen de la organización.

9.1.7 Medio, bajo y despreciable Para el desarrollo del proyecto, los activos dentro de estos niveles de riesgo serán analizados puntualmente en las amenazas que tengan niveles más altos.

9.2 ANALISIS DE ACUERDO CON LAS AMENAZAS

- [A.3] Manipulación de los registros de actividad (Logs)
    - Activos - dimensiones afectados – nivel de riesgo.
        - [B][IS][D] Base de datos operativa – Integridad – Alto.
    - Incidencias relacionadas.
        - Insuficiente gestión de controles de acceso.
        - Mal uso de usuarios y contraseñas.

- [A.4] Manipulación de ficheros de configuración.
    - -Activos - dimensiones afectados – nivel de riesgo.
        - [A][HW] Servidores – Disponibilidad / Integridad / Confidencialidad – Catástrofe.
    - Incidencias.
        - Insuficiente control de los ficheros de configuración.
        - Insuficiente gestión de controles de acceso.
        - Mal uso de usuarios y contraseñas.

- [A.5] Suplantación de identidad.
    - Activos - dimensiones afectados – nivel de riesgo.
        - [B][S]Servicio Telefonía - Integridad / Confidencialidad / Autenticidad – Catástrofe.
        - [B][S] Red Lan Operativa Voz y Datos – Integridad / Confidencialidad / Autenticidad – Alto.

        - [A][SS] Servicio de líneas móviles – Integridad / Confidencialidad / Autenticidad – Catástrofe.
    - Incidencias.
        - Insuficiente gestión de controles de acceso a los servicios de telefonía y la red LAN.
        - Insuficiente control sobre puntos de red no utilizados.
        - Equipos móviles sin PIN de acceso con clave muy simple.
        - Control insuficiente de acceso a internet.

- [A.6] Abuso de privilegios de acceso

    - Activos - dimensiones afectados – nivel de riesgo.
        - [A][L] Centro de datos - Disponibilidad – Catástrofe.
        - [A][L] Locaciones operativas y administrativas – Disponibilidad – Catástrofe.
    - Incidencias.
        - Insuficiente gestión de controles de acceso a las instalaciones.
        - Las zonas comprometidas no cuentan con suficientes mecanismos de control de acceso.
        - El acceso a las zonas comprometidas permite manipulación de equipos, archivos, etcétera.

- [A.7] Uso no previsto.

    - Activos - dimensiones afectados – nivel de riesgo.
        - [B][S]Servicio Telefonía – Disponibilidad / Integridad Confidencialidad – Catástrofe.
        - [B][S] Red LAN Operativa Voz y Datos – Disponibilidad / Integridad / Confidencialidad – Catástrofe.
        - [A][SS] Servicio de líneas móviles – Disponibilidad / Integridad / Confidencialidad – Muy Alto.
        - [A][L] Locaciones operativas y administrativas – Disponibilidad – Muy Ato.
        - [A][HW] Equipos de telefonía móvil - – Disponibilidad / Integridad / Confidencialidad – Crítico.
        - [A][AUX] Sistema de alimentación ininterrumpido – Disponibilidad – Crítico.
        - [A][AUX] Cableado fibra óptica – Disponibilidad / Integridad / Confidencialidad – Muy Alto.
        - [A][COM] Canal de internet principal y backup - Disponibilidad / Integridad / Confidencialidad – Catástrofe.
        - [A][COM] Canal de MPLS casa matriz Ppal y BCK - Disponibilidad / Integridad / Confidencialidad – Catástrofe.

        - [A][IS] Servicio de servidor de archivos - Disponibilidad / Integridad / Confidencialidad – Catástrofe.
    - Incidencias.
        - Problemas de capacitación del personal en el uso de las tecnologías y/o políticas de seguridad.
        - Insuficiente gestión de controles de acceso a recursos de internet, servidor de archivos, equipos de telefonía móvil.
        - Insuficiente gestión de encriptación de equipos y/o información.
        - Actividades de teletrabajo no controlado.
        - Mala gestión de medios extraíbles.
        - Mala gestión en la instalación de software.

- [A.8] Difusión de software dañino.

    - Activos - dimensiones afectados – nivel de riesgo.
        - [B][S]Servicio Telefonía - Disponibilidad / Integridad / Confidencialidad – Catástrofe.
        - [B][S] Servicio de gestión de marcación telefónica - Disponibilidad / Integridad / Confidencialidad – Crítico.
        - [A][SW] Software ofimático- Disponibilidad / Integridad / Confidencialidad – Catástrofe.
        - [A][SW] Software antivirus- Disponibilidad / Integridad / Confidencialidad – Extremadamente Crítico.
        - [A][SW] Software administrativo-contabilidad-rrhh- Disponibilidad / Integridad / Confidencialidad – Catástrofe.
        - [A][HW] Equipos de escritorio - laptops- Disponibilidad / Integridad / Confidencialidad – Catástrofe.
        - [A][HW] Servidores- Disponibilidad / Integridad / Confidencialidad – Catástrofe.
        - [A][HW] Equipos de telefonía móvil- Disponibilidad / Integridad / Confidencialidad – Catástrofe.
        - [A][COM] Firewall- Disponibilidad / Integridad / Confidencialidad – Crítico.
    - Incidencias
        - Mala gestión de antivirus (o ausencia de este) en equipos.
        - Insuficiente control de acceso a Internet.
        - Insuficiente gestión de medios extraíbles.

- [A.11] Acceso no autorizado.

    - Activos - dimensiones afectados – nivel de riesgo.
        - [B][S]Servicio Telefonía – Integridad / Confidencialidad / Autenticidad – Catástrofe.

        - [B][S] Red Lan Operativa Voz y Datos – Integridad / Confidencialidad – Catástrofe.
        - [B][IS][D] Base de datos operativa – Integridad / Confidencialidad – Catástrofe.
        - [A][SS] Servicio de líneas móviles – Integridad / Confidencialidad / Autenticidad – Catástrofe.
        - [A][HW] Equipos de escritorio – laptops – Disponibilidad / Integridad / Confidencialidad – Catástrofe.
        - [A][HW] Equipos de telefonía móvil – Disponibilidad / Integridad / Confidencialidad – Catástrofe.
        - [A][AUX] Servicio Backups – Integridad / Confidencialidad / Autenticidad – Catástrofe.
        - [A][COM] Canal de internet principal y backup – Integridad / Confidencialidad / Autenticidad – Alto.
        - [A][COM] Canal de MPLS casa matriz Ppal y BCK – Integridad / Confidencialidad / Autenticidad - Extremadamente Crítico.
        - [A][COM] Cableado estructura voz y datos – Integridad / Confidencialidad / Autenticidad – Extremadamente Crítico.
    - Incidencias
        - Problemas de capacitación de personal, la rotación alta afecta en los niveles de capacitación en tecnología y/o políticas de seguridad.
        - Insuficiente gestión de controles de acceso.
        - Insuficientes políticas en gestión de usuarios y contraseñas.
        - Actividades de teletrabajo no controlado.
        - Insuficiente gestión de encriptación de equipos.
        - Control insuficiente de acceso a internet.
        - Mala gestión de equipos desatendidos.
        - Mala gestión de medios extraíbles.

- [A.12] Análisis de tráfico

    - Activos - dimensiones afectados – nivel de riesgo.
        - [B][S] Red Lan Operativa Voz y Datos – Confidencialidad / Autenticidad – Alto.
        - [A][COM] Canal de MPLS casa matriz Ppal y BCK – Confidencialidad – Alto.
    - Incidencias.
        - Redes WIFI no protegidas.
        - Redes LAN (puertos libres) no protegidos.
        - Insuficiente gestión de encriptación de información.

- [A.13] Repudio (Negación de actuaciones).

    - Activos - dimensiones afectados – nivel de riesgo.

        - [B][S]Servicio Telefonía – Trazabilidad – Desastre.
        - [A][AUX] Servicio Backups – Trazabilidad – Catástrofe .
        - [A][COM] Canal de internet principal y backup – Trazabilidad – Alto.
        - [A][COM] Canal de MPLS casa matriz Ppal y BCK – Trazabilidad - Extremadamente Crítico.
    - Incidencias.
        - Control insuficiente de acceso a internet.
        - Gestión insuficiente de los logs de actividades.
        - Gestión insuficiente de control de acceso.

- [A.14] Interceptación de información (escucha)

    - Activos - dimensiones afectados – nivel de riesgo.
        - [A][COM] Canal de MPLS casa matriz Ppal y BCK – Confidencialidad – Alto.
    - Incidencias.
        - Gestión insuficiente de encriptación de información.

- [A.15] Modificación de la información.

    - Activos - dimensiones afectados – nivel de riesgo.
        - [B][S]Servicio Telefonía – Integridad – Muy Alto.
        - [A][P] Personal operativo – Integridad – Alto.
        - [A][P] Personal administrativo RRHH\Finanzas\Gerencia – Integridad - Extremadamente Crítico.
        - [A][P] Personal estructura operativa – Integridad – Alto.
        - [A][SS] Servicio de correo electrónico – Integridad – Alto.
        - [A][HW] Servidores – Integridad – Catástrofe.
        - [A][AUX] Servicio Backups – Integridad – Catástrofe.
        - [A][IS] Servicio de servidor de archivos – Integridad – Catástrofe.
    - Incidencias.
        - Falta control sobre recursos de archivos.
        - Falta gestión de encriptación de información.
        - No se implementan firmas digitales.
        - Problemas de capacitación de personal.
        - Mala gestión de medios extraíbles.
        - Control insuficiente de acceso a internet.

- [A.18] Destrucción de la información.
    - Activos - dimensiones afectados – nivel de riesgo.
        - [B][S]Servicio Telefonía – Disponibilidad – Crítico.
        - [B][S] Red Lan Operativa Voz y Datos – Disponibilidad – Crítico.
        - [A][P] Personal operativo – Disponibilidad – Alto.
    - Incidencias.

        - Fallas en controles de acceso.
        - Falta de capacitación.

- [A.19] Revelación de la información.

    - Activos - dimensiones afectados – nivel de riesgo.
        - [B][S]Servicio Telefonía – Confidencialidad – Alto.
        - [A][P] Personal operativo – Confidencialidad – Catástrofe.
        - [A][P] Personal administrativo RRHH\Finanzas\Gerencia – Confidencialidad – Catástrofe.
        - [A][P] Personal estructura operativa – Confidencialidad - Muy Alto.
        - [A][SS] Servicio de correo electrónico – Confidencialidad – Alto.
    - Incidencias
        - Problemas de capacitación del personal.
        - Problemas de alta rotación del personal.
        - Control insuficiente de acceso a internet.
        - Gestión insuficiente de encriptación de información.

- [A.20] Ingeniería Social.

    - Activos - dimensiones afectados – nivel de riesgo.
        - [A][P] Personal operativo – Disponibilidad / Integridad / Confidencialidad – Catástrofe.
        - [A][P] Personal administrativo RRHH\Finanzas\Gerencia - Disponibilidad / Integridad / Confidencialidad - Extremadamente Crítico.
        - [A][P] Personal estructura operativa - Disponibilidad / Integridad / Confidencialidad – Extremadamente Crítico.
    - Incidencias.
        - Problemas de capacitación del personal.

- [A.22] Manipulación de programas.

    - Activos - dimensiones afectados – nivel de riesgo.
        - [B][S]Servicio Telefonía – Disponibilidad / Integridad / Confidencialidad – Catástrofe.
        - [B][S] Servicio de gestión de marcación telefónica – Disponibilidad / Integridad / Confidencialidad – Catástrofe.
        - [A][SW] Software ofimático – Disponibilidad / Integridad / Confidencialidad – Alto.
        - [A][SW] Software antivirus – Disponibilidad / Integridad / Confidencialidad – Alto.
        - [A][SW] Software administrativo-contabilidad-rrhh – Disponibilidad / Integridad / Confidencialidad – Desastres.

        - [A][HW] Equipos de escritorio – laptops –– Disponibilidad / Integridad / Confidencialidad - Extremadamente Crítico.
        - [A][HW] Equipos de telefonía móvil - Disponibilidad / Integridad / Confidencialidad – Catástrofe.
    - Incidencias.
        - Mala gestión de antivirus (o ausencia de este).
        - Insuficiente control de acceso a aplicaciones o mala gestión de permisos.
        - Problemas de capacitación del personal.
        - Documentación deficiente del software.

- [A.23] Manipulación del Hardware.

    - Activos - dimensiones afectados – nivel de riesgo.
        - [A][HW] Equipos de escritorio – laptops – Disponibilidad – Catástrofe.
        - [A][AUX] Sistema de alimentación ininterrumpido – Disponibilidad – Crítico.
        - [A][AUX] Generador eléctrico de respaldo – Disponibilidad -Muy Alto.
        - [A][AUX] Cableado eléctrico Centro – Disponibilidad - Muy Alto.
        - [A][AUX] Cableado fibra óptica - Disponibilidad – Catástrofe.
        - [A][COM] Switches Core y Distribuidores – Disponibilidad – Catástrofe.
    - Incidencias.
        - Insuficientes medidas de seguridad para proteger los componentes físicos de hardware.
        - Mejorar control de acceso físico y actividades de mantenimiento de equipos críticos.
        - Mejorar control de acceso a zonas críticas.

- [A.24] Denegación de servicio.

    - Activos - dimensiones afectadas – nivel de riesgo.
        - [B][S] Red Lan Operativa Voz y Datos - Disponibilidad – Catástrofe.
        - [A][SS] Servicio de página web - Disponibilidad – Crítico.
        - [A][HW] Servidores - Disponibilidad – Catástrofe.
        - [A][AUX] Servicio Backups – Disponibilidad - Muy Alto.
        - [A][COM] Switches Core y Distribuidores – Disponibilidad - Catástrofe.
        - [A][COM] Canal de internet principal y backup – Disponibilidad- Extremadamente Crítico.
        - [A][COM] Canal de MPLS casa matriz Ppal y BCK – Disponibilidad - Extremadamente Crítico.
        - [A][COM] Cableado estructura voz y datos – Disponibilidad – Catástrofe.

        - [A][IS] Servicio de base de datos administrativa – Disponibilidad - Extremadamente Crítico.
    - Incidencias.
        - Actividades de teletrabajo no controlado.
        - Control insuficiente de acceso a internet.
        - Recursos insuficientes para gestionar actividades de teletrabajo e internas.
        - Recursos insuficientes en servidores.
        - Insuficiente gestión de los cronogramas de mantenimiento.

- [A.25] Robo de equipos.

    - Activos - dimensiones afectadas – nivel de riesgo.
        - [A][HW] Equipos de telefonía móvil.
    - Incidencias.
        - Actividades de teletrabajo no controlado.
        - Ausencia o mala gestión de backups.
        - Mal uso de usuarios y contraseñas.
        - Insuficiente gestión de encriptación de equipos.
        - Mala gestión de medios extraíbles.
        - Insuficiente gestión\control de equipos móviles.

- [A.28] Indisponibilidad del personal.

    - Activos - dimensiones afectadas – nivel de riesgo.
        - [A][P] Personal operativo – Disponibilidad - Catástrofe.
        - [A][P] Personal estructura operativa – Disponibilidad – Alto.
    - Incidencias
        - Problemas de alta rotación del personal, ausencia.
        - Problemas de capacitación de personal.

- [A.29] Extorsión.

    - Activos - dimensiones afectadas – nivel de riesgo.
        - [A][P] Personal operativo – Disponibilidad / Integridad / Confidencialidad – Alto.
        - [A][P] Personal administrativo RRHH\Finanzas\Gerencia – Disponibilidad / Integridad / Confidencialidad – Alto.
        - [A][P] Personal estructura operativa – Disponibilidad / Integridad / Confidencialidad.
    - Incidencias.
        - Problemas en capacitación del personal.
        - Insuficiente encriptación de información y dispositivos.
        - Insuficiente gestión de medios extraíbles.

- [E.1] Errores de los usuarios.
    - Activos - dimensiones afectadas – nivel de riesgo.
        - [A][AUX] Servicio Backups – Disponibilidad / Integridad / Confidencialidad - Muy Alto.
        - [A][IS] Servicio de servidor de archivos – Disponibilidad / Integridad / Confidencialidad – Catástrofe.
    - Incidencias
        - Ausencia o mala gestión de backups.
        - Problemas en capacitación del personal.
        - Insuficiente gestión de logs.

- [E.2] Errores del administrador del sistema/de la seguridad.
    - Activos - dimensiones afectadas – nivel de riesgo.
        - [A][HW] Servidores – Disponibilidad / Integridad / Confidencialidad – Catástrofe.
    - Incidencias.
        - Ausencia o mala gestión de backups.
        - Problemas en capacitación del personal.
        - Insuficiente gestión de logs.

- [E.3] Errores de monitorización (log).
    - Activos - dimensiones afectadas – nivel de riesgo.
        - [B][IS][D] Base de datos operativa – Integridad – Catástrofe.
        - [A][HW] Servidores – Integridad – Muy Alto.
    - Incidencias.
        - Insuficiente gestión de logs.
        - No hay políticas para la gestión y revisión de logs.

- [E.8] Difusión de software dañino.
    - Activos - dimensiones afectadas – nivel de riesgo.
        - [A][SW] Software ofimático – Disponibilidad / Integridad / Confidencialidad – Muy Alto.
        - [A][SW] Software administrativo-contabilidad-rrhh – Disponibilidad / Integridad / Confidencialidad – Catástrofe.
        - [A][HW] Equipos de escritorio – laptops – Disponibilidad / Integridad / Confidencialidad – Catástrofe.
        - [A][HW] Servidores – Disponibilidad / Integridad / Confidencialidad – Catástrofe.

        - [A][HW] Equipos de telefonía móvil – Disponibilidad / Integridad / Confidencialidad – Catástrofe.
        - [A][COM] Firewall – Disponibilidad / Integridad / Confidencialidad – Catástrofe.
    - Incidencias.
        - Mala gestión de antivirus (o ausencia de este).
        - Problemas en capacitación de personal.

- [E.15] Alteración de Información.

    - Activos - dimensiones afectadas – nivel de riesgo.
        - [B][IS][D] Base de datos operativa – Integridad – Crítico.
        - [A][P] Personal operativo – Integridad – Extremadamente Crítico.
        - [A][IS] Servicio de servidor de archivos – Integridad – Alto.
    - Incidencias.
        - Problemas de capacitación de personal.
        - Mala gestión de medios extraíbles.
        - Control insuficiente de acceso a internet.
        - Insuficiente gestión\aplicación de firmas digitales y encriptación.
        - Problemas de control de acceso.

- [E.18] Destrucción de la información.

    - Activos - dimensiones afectadas – nivel de riesgo.
        - [A][P] Personal operativo – Disponibilidad – Alto.
    - Incidencias.
        - Problemas de capacitación del personal.
        - Ausencia o mala gestión de backups.
        - Mala gestión de medios extraíbles.
        - Control insuficiente de acceso a internet.
        - Insuficiente gestión de control de acceso.

- [E.19] Fugas de información.

    - Activos - dimensiones afectadas – nivel de riesgo.
        - [B][IS][D] Base de datos operativa – Confidencialidad – Catástrofe.
        - [A][P] Personal estructura operativa – Confidencialidad - Muy Alto.
        - [A][SS] Servicio de líneas móviles – Confidencialidad – Catástrofe.
        - [A][IS] Servicio de servidor de archivos – Confidencialidad – Extremadamente Crítico.
    - Incidencias.
        - Problemas de alta rotación de personal.
        - Problemas de capacitación del personal.
        - Actividades de teletrabajo no controlado.

        - Control insuficiente de acceso a internet.
        - Mala gestión de medios extraíbles.
        - Insuficiente gestión de encriptación.

- [E.20] Vulnerabilidades de los programas (Software).

    - Activos - dimensiones afectadas – nivel de riesgo.
        - [B][S] Servicio de gestión de marcación telefónica – Disponibilidad / Integridad / Confidencialidad – Catástrofe.
        - [A][HW] Equipos de escritorio – laptops - Disponibilidad / Integridad / Confidencialidad – Catástrofe.
        - [A][HW] Servidores - Disponibilidad / Integridad / Confidencialidad – Crítico.
        - [A][COM] Firewall – Disponibilidad / Integridad / Confidencialidad – Crítico.
    - Incidencias.
        - Mala gestión de antivirus (o ausencia de este).
        - Falta de gestión de actualizaciones.

- [E.21] Errores de mantenimiento\actualización de programas.

    - Activos - dimensiones afectadas – nivel de riesgo.
        - [B][S] Servicio de gestión de marcación telefónica – Disponibilidad / Integridad – Catástrofe.
        - [A][HW] Equipos de escritorio – laptops – Disponibilidad / Integridad – Catástrofe.
        - [A][HW] Servidores – Disponibilidad / Integridad – Catástrofe.
        - [A][COM] Firewall – Disponibilidad / Integridad – Catástrofe.
    - Incidencias.
        - Mala gestión de antivirus (o ausencia de este).
        - Falta de gestión de actualizaciones.
        - Mala gestión de mantenimiento de equipos.

- [E.23] Errores de mantenimiento\actualización de hardware.

    - Activos - dimensiones afectadas – nivel de riesgo.
        - [A][HW] Equipos de escritorio – laptops – Disponibilidad – Catástrofe.
        - [A][AUX] Sistema de alimentación ininterrumpido – Disponibilidad – Crítico.
        - [A][AUX] Generador eléctrico de respaldo – Disponibilidad - Muy Alto.
        - [A][AUX] Cableado fibra óptica – Disponibilidad – Catástrofe.
        - [A][COM] Switches Core y Distribuidores – Disponibilidad - Muy Alto.
        - [A][COM] Firewall – Disponibilidad – Catástrofe.
    - Incidencias.

        - Características de los equipos son insuficientes.
        - Mala gestión de mantenimiento de equipos.

- [E.24] Caída del sistema por agotamiento de recursos.

    - Activos - dimensiones afectadas – nivel de riesgo.
        - [B][S] Red Lan Operativa Voz y Datos – Disponibilidad – Crítico.
        - [A][HW] Equipos de escritorio – laptops – Disponibilidad - Catástrofe
        - [A][HW] Servidores – Disponibilidad – Catástrofe.
        - [A][COM] Switches Core y Distribuidores – Disponibilidad - Muy Alto
        - [A][COM] Firewall – Disponibilidad – Catástrofe.
        - [A][COM] Canal de internet principal y backup – Disponibilidad - Extremadamente Crítico.
        - [A][COM] Canal de MPLS casa matriz Ppal y BCK – Disponibilidad - Extremadamente Crítico.
        - [A][COM] Cableado estructura voz y datos – Disponibilidad – Catástrofe.
    - Incidencias
        - Características de los equipos son insuficientes.
        - Mala gestión de mantenimiento de equipos.
        - Control insuficiente de acceso a internet.
        - Mala gestión de medios extraíbles.

- [E.25] Perdida de equipos.

    - Activos - dimensiones afectadas – nivel de riesgo.
        - [A][HW] Equipos de telefonía móvil – Disponibilidad / Confidencialidad – Crítico.
    - Incidencias.
        - Actividades de teletrabajo no controlado.
        - Insuficiente gestión de encriptación de equipos.
        - Ausencia o mala gestión de backups.

- [E.28] Indisponibilidad del personal.

    - Activos - dimensiones afectadas – nivel de riesgo.
        - [A][P] Personal operativo – Disponibilidad – Catástrofe.
    - Incidencias.
        - Problemas de alta rotación del personal, ausencias.

- [I.*] Desastre Industriales.

    - Activos - dimensiones afectadas – nivel de riesgo.

        - [A][L] Locaciones operativas y administrativas – Disponibilidad – Catástrofe.
        - [A][AUX] Cableado eléctrico Centro – Disponibilidad – Catástrofe.
    - Incidencias.
        - Ausencia o mala gestión de backups.
        - Falta de plan de contingencia.
        - Insuficientes equipos de detección y protección.

- [I.2] Daños por agua.

    - Activos - dimensiones afectadas – nivel de riesgo .
        - [A][L] Edificio General – Disponibilidad - Extremadamente Crítico.
        - [A][L] Locaciones operativas y administrativas – Disponibilidad - Extremadamente Crítico.
        - [A][HW] Equipos de escritorio – laptops – Disponibilidad – Medio.
        - [A][HW] Equipos de telefonía móvil – Disponibilidad – Crítico.
    - Incidencias.
        - Ausencia o mala gestión de backups.
        - Falta de plan de contingencia.
        - Insuficientes equipos de detección y protección.

- [I.3] Contaminación medioambiental.

    - Activos - dimensiones afectadas – nivel de riesgo.
        - [A][L] Edificio General – Disponibilidad – Catástrofe.
        - [A][L] Centro de datos – Disponibilidad – Catástrofe.
        - [A][AUX] Generador eléctrico de respaldo – Disponibilidad - Muy Alto.
        - [A][AUX] Cableado fibra óptica – Disponibilidad - Muy Alto.
        - [A][AUX] Servicio Backups – Disponibilidad - Muy Alto.
        - [A][COM] Switches Core y Distribuidores – Disponibilidad - Muy Alto.
        - [A][COM] Firewall – Disponibilidad – Crítico.
    - Incidencias.
        - Ausencia o mala gestión de backups.
        - Falta de plan de contingencia.
        - Insuficientes equipos de detección y protección.

- [I.4] Contaminación electromagnética.

    - Activos - dimensiones afectadas – nivel de riesgo.
        - [A][L] Edificio General – Disponibilidad – Catástrofe.
        - [A][L] Centro de datos – Disponibilidad – Catástrofe.
        - [A][AUX] Servicio Backups – Disponibilidad – Catástrofe.
        - [A][COM] Firewall – Disponibilidad – Crítico.
    - Incidencias.

        - Ausencia o mala gestión de backups.
        - Mala gestión de medios extraíbles.

- [I.5] Avería de origen físico o lógico.

    - Activos - dimensiones afectadas – nivel de riesgo.
        - [B][S]Servicio Telefonía – Disponibilidad – Crítico.
        - [B][S] Servicio de gestión de marcación telefónica – Disponibilidad – Crítico.
        - [A][SW] Software antivirus – Disponibilidad – Alto.
        - [A][SW] Software administrativo-contabilidad-rrhh – Disponibilidad – Muy Alto.
        - [A][HW] Equipos de escritorio – laptops – Disponibilidad – Catástrofe.
        - [A][HW] Servidores – Disponibilidad – Catástrofe.
        - [A][AUX] Servicio Backups – Disonibilidad – Catástrofe.
    - Incidencias.
        - Ausencia o mala gestión de backups.
        - Mala gestión de antivirus (o ausencia de este).
        - Características de los equipos son insuficientes.
        - Mala gestión de mantenimiento de equipos.
        - Mala gestión de medios extraíbles.

- [I.7] Condiciones inadecuadas de temperatura o humedad.

    - Activos - dimensiones afectadas – nivel de riesgo.
        - [A][HW] Equipos de escritorio – laptops – Disponibilidad – Muy Alto.
        - [A][HW] Equipos de telefonía móvil – Disponibilidad – Catástrofe.
        - [A][AUX] Servicio Backups – Disponibilidad – Catástrofe.
    - Incidencias.
        - Condiciones físicas inadecuadas.
        - Mala gestión de medios extraíbles.
        - Insuficientes equipos de detección y protección.
        - Problemas de capacitación de personal.

- [I.8] Fallo de servicios de comunicaciones.

    - Activos - dimensiones afectadas – nivel de riesgo.
        - [B][S] Red Lan Operativa Voz y Datos – Disponibilidad – Crítico.
        - [B][S]Servicio Telefonía – Disponibilidad – Catástrofe.
        - [A][COM] Canal de internet principal y backup – Disponibilidad – Extremadamente Crítico.
        - [A][COM] Canal de MPLS casa matriz Ppal y BCK – Disponibilidad – Extremadamente Crítico.
    - Incidencias.

        - Actividades de teletrabajo no controlado.
        - Insuficientes sistemas de monitoreo.

- [N.2] Daños por agua.

    - Activos - dimensiones afectadas – nivel de riesgo.
        - [A][L] Edificio General – Disponibilidad - Extremadamente Crítico.
        - [A][L] Locaciones operativas y administrativas – Disponibilidad - Extremadamente Crítico.
        - [A][HW] Equipos de telefonía móvil – Disponibilidad – Crítico.
        - [A][AUX] Sistema de alimentación ininterrumpido – Disponibilidad – Catástrofe.
    - Incidencias.
        - Ausencia o mala gestión de backups.
        - Insuficientes equipos de detección y protección.

10 SALVAGUARDAS

El proceso de selección de salvaguardas (apoyado en el aplicativo PILAR y MAGERIT) permite seleccionar una serie de medidas (políticas y controles) que se han considerado como oportunas y necesarias para los problemas detectados. Es importante señalar que las políticas serán desarrolladas en el capítulo correspondiente al diseño del SGSI.

Se completar la información se agrega además una calificación de acuerdo con lo que se ha podido identificar actualmente el nivel de madurez de la salvaguarda (puesto que en algunos casos la organización ha aplicado medidas) según la siguiente tabla:

Cuadro 13.Nivel de madurez de salvaguardas

Nivel	Descripción
L0	Inexistente
L1	Inicial
L2	Reproducible, intuitivo
L3	Proceso definido
L4	Gestionado y medible
L5	Optimizado

Fuente: Propia

Las salvaguardas seleccionadas son las siguientes:

Cuadro 14. Salvaguardas seleccionadas

SECCIÓN	ITEM	SALVAGUARDA	MAD
[IA] Identificación y autenticación	Factores de autenticación	Uso de Contraseña	L3
		Biometría	L0
	Canal Seguro de Autenticación		L0
	Cuentas Especiales (Administración)	Cuentas especiales para administradores de seguridad	L0
		Cuentas especiales para administradores del sistema	L3
		Cuentas especiales para actividades de auditoría	L0
[AC] Control de Acceso Lógico	Segregación de tareas	Separación de responsabilidades de administración y operación	L1

[D] Protección de la información	Inventario de activos de información	Actualización regular del inventario	L2
		Identificación del propietario	L2
	Protección de la confidencialidad	Cifrado de la información	L0
	Uso de firmas electrónicas	Normativa sobre firma electrónica	L0
		Mecanismo de firma electrónica	L0
	Copias de seguridad	Normativa copias de seguridad	L2
		Procedimientos tareas de realización de copias se seguridad	L2
		Gestión de las copias de seguridad	L2
		Protección de las copias de seguridad	L2
[K] Protección de claves criptográficas	Gestión de claves de firma de información		L0
	Gestión de claves para contenedores criptográficos		L0
	Gestión de claves de comunicaciones		L0
[S] Protección de los servicios	Pruebas en preproducción		L2
	Pruebas de aceptación		L2
	Pruebas de regresión		L1
	Teletrabajo	Identificación de los riesgos	L1
		Determinación de métodos de acceso autorizados	L1
		Se dispone de normativa para la autorización del acceso y concesión de privilegios	L1
		Se garantiza el derecho para controlar (y suspender en su caso) la actividad de los usuarios	L1
		Acuerdos para intercambio de información y uso de software y hardware	L1
[SW] Protección de las aplicaciones informáticos	Administración	Inventario de aplicaciones	L1
		Se protegen los derechos de propiedad intelectual	L1
	Perfiles de Seguridad	Eliminación o modificación de las cuentas estándar de administración	L2
		Protocolo de modificación de configuración	L2

	Cambios	Priorización de actualizaciones encaminadas a corregir riesgos elevados	L2
[HW] Protección de los equipos informáticos	Perfiles de seguridad	Solo administradores autorizados para modificar configuración	L3
		Funciones activadas de forma segura	L2
[COM] Protección de las comunicaciones	Perfiles de seguridad	Eliminación\modificación de las cuentas estándar de administrador	L2
		Solo administradores pueden modificar la configuración	L2
		Servicios activados se configuran de forma segura	L2
	Protección criptográfica de la confidencialidad de la información		L1
	Seguridad Wireless	Se eliminan claves por defecto	L3
		Se deshabilitan protocolos de gestión no esenciales	L2
[MP] Soportes de información	Administración	Normativa relativa a soportes de información	L2
		Procedimientos relativos a soportes de información	L2
		Inventario de soportes	L2
	Gestión de soportes	Manejo	L3
	Etiquetado		L0
	Seguridad de los soportes fuera de las instalaciones	Registro de entradas y salidas	L2
		Protección del soporte técnicamente antes de la salida	L2
		Revisión del soporte a su regreso	L2
	Protección criptográfica de la información	Cifrado del contenido	L0
		Firmado del contenido	L0
[L] Protección de las instalaciones	Inventario de las instalaciones		L2
	Protección frente a desastres		L4
	Continuidad de operaciones		L1
	Protección de las áreas de carga y despacho		L2
[PS] Gestión del personal	Condiciones Contractuales		L3
	Formación continua		L3
	Personal subcontratado		L3
	Actuación frente a código dañino		L2
	Coordinación con otros sistemas de información afectados		L2
	Se suspende cautelarmente los trabajos en el sistema afectado		L2

[IR] Gestión de incidentes	Se aísla cautelarmente el sistema afectado	L2
	Comunicación con los afectados por el incidente (internos y externos)	L2
	Evaluación y calificación de los eventos de seguridad	L1
[Tools] Herramientas de seguridad	Herramientas contra código dañino	L4
	Herramienta de detección\prevención de intrusión	L4
[A] Registro y Auditoría	Administración	L1
	Herramientas	L1
	Información	L1
	Actividades	L1
[E] Relaciones Externas	Se dispone de normativa relativa a la continuidad del negocio	L2
	Se ha realizado análisis de impacto	L2
	Actividades preparatorias	L2
	Reacción, todas las áreas de la organización están coordinadas	L2
	Plan de recuperación de desastres	L1

Fuente: Propia

11 ROLES Y RESPONSABILIDADES

Con el fin de facilitar el éxito de una futura implementación del SGSI que se está diseñando en el actual proyecto es importante considerar los diferentes roles y responsabilidades que tendrán las personas que intervengan o se relacionen con el sistema.

Dentro del SGSI se identifican los siguientes actores:

- Propietario: En este caso se hace referencia al dueño del activo de información, sea este los datos o los dispositivos por medio de los cuales se procesan o almacenan, el cual debe estar debidamente identificado y registrado. Es importante considerar que el propietario puede ser interno o externo, puesto que en un Centros de Contacto se suele trabajar con datos de los clientes para los cuales se brinda el servicio, y en el caso interno se trata de la organización o de las áreas (El departamento de contabilidad será, normalmente, el propietario de la información financiera sin desconocer que existe un nivel superior con mayor propiedad sobre dichos datos).

- Encargado: Si bien existe un propietario del activo de información puede haber otras personas que se encargan de realizar acciones sobre este, o también la persona que ejecuta el procedimiento, control o política.

- Consultor: Actores que no necesariamente son dueños ni actúan sobre el activo de información, pero tienen el conocimiento necesario para la correcta gestión del SGSI.

Dentro de los roles se definen los siguientes:

- Comité Directivo: Es el máximo nivel organización de la Empresa, agrupando los directores de cada área. Encargados de las decisiones a nivel estratégico de toda la organización. Son los responsables de la gestión de recursos para el Sistema de Gestión de Seguridad de la Información y de la aprobación de las políticas de seguridad y los planes de continuidad del SGSI y de la organización en general.

- Comité de Seguridad: Integra las personas designadas por el Comité Directivo, el responsable del SGSI y los consultores. Realiza la gestión del plan de implementación del SGSI, la toma de decisiones sobre las políticas de seguridad de la información y la distribución de los recursos.

- Responsable de SGSI: Rol encargado de la gestión a nivel estratégico del SGSI, siendo responsable de la implementación de la política de seguridad de la información, así como su mejora continua, la gestión de los incidentes de seguridad, de buscar el cumplimiento del sistema y del apoyo del Comité Directivo y del Comité de Seguridad. En el caso de Telemarketing S.A.S corresponde al Jefe de TI, lo cual implica que hace parte tanto del Comité Directivo como del Comité de Seguridad, teniendo a su cargo las responsabilidades que se extienden de ambos grupos.

  Como jefe de TI es responsable la administración de la infraestructura tecnológica de la organización y la planeación estratégica a nivel de TI y el apoyo en la toma de decisiones para el Comité Directivo.

- Equipo de seguridad: Corresponde al equipo de apoyo al Responsable del SGSI para la aplicación y cumplimiento de las políticas y controles de seguridad establecidos. Este papel, para Telemarketing S.A.S lo cumple el Departamento de TI.

  En relación con el SGSI se encargan del cumplimiento de las políticas, controles y procedimientos, el respaldo de la información, el control de la instalación de las aplicaciones, el cumplimiento de los cronogramas de mantenimiento, entre otros.

  A nivel de TI están encargados de las actividades de apoyo operativo de la organización como el soporte técnico, desarrollos internos, gestión del software de la organización, entre otros.

Existen en la organización otros roles que, dado el alcance del proyecto, no se han descrito en relación del SGSI, pero que pueden intervenir (o verse afectados) por el Sistema de Gestión de Seguridad de la Información, como son:

- Director y Equipo de Gestión de Talento Humano: Equipo encargado de la gestión del recurso humano. Dentro de sus funciones se encuentra la contratación y gestión del personal, gestión de las hojas de vida, cumplimiento de las obligaciones legales en materia de recursos humanos.

- Director y Equipo Financiero y Compras: Departamento encargado de todas las acciones financieras de la compañía, entre ellas las obligaciones financieras, pagos de proveedores, pago de empleados. En la gestión de compras están encargados de la gestión de proveedores, calificación de estos y ejecución de las compras requeridas por la empresa.

- Director y Equipo de Calidad: Esta área está enfocada en la operación de la empresa, velando por que las actividades cumplan con los requerimientos de los clientes y estándares establecidos para la prestación de servicios.

- Director y Equipo de Formación: El área de formación es la encargada de dar la capacitación al personal de la empresa. Es el primer contacto (a nivel operativo) de los ejecutivos de *Contact Center* con la organización, pero además durante la vigencia de contrato recibirán formaciones de refuerzo y actualización por parte de este departamento.

- Equipo Operativo:

    - Director Operativo: Persona encargada de la gestión y administración de los proyectos que se ejecutan en la empresa (en generar son los servicios que se brindan a los clientes).

    - Jefes de Proyectos: Persona responsable de gestionar y administrar un único proyecto. Deben procurar el correcto avance del proyecto.

    - Supervisores de Proyectos: Son los encargados de gestionar el global de agentes del proyecto. Cuando un proyecto se compone de subproyectos, los supervisores son responsables de cada subproyecto.

    - Coordinadores de Proyectos: Los proyectos de atienden por grupos de agentes en un número no mayor a 12 personas por grupo. Cada Coordinador es responsable de cada grupo, de que estas personas cumplan con las directrices de la empresa.

    - Agentes. Constituyen el contacto directo con el cliente, son los ejecutores de la operación y por ende, son la mayor fuerza (en cuanto a cantidad de personas) dentro de la organización.

12 DISEÑO SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Un sistema de gestión de seguridad de la información se puede describir como un conjunto de políticas o normas (incluso controles) que sirven como lineamientos para la protección, la gestión o la administración de la información y de los activos que la procesan, almacenan o transportan.

El diseño del SGSI contempla los siguientes puntos:

- El alcance del sistema, es decir, determinar que abarca el SGSI dentro de la organización, hasta donde llega, quienes deben incluirlo en sus procesos.
- La política general seguridad de la información, en la cual se definen:
    - Los compromisos de la organización frente al SGSI.
    - Los requisitos que cumple y,
    - Los objetivos.
- Política de seguridad a seguir, aquí se definen las diferentes políticas que componen el SGSI.
- Concienciación y formación del personal.

12.1 ALCANCE

El Sistema de Gestión de Seguridad de la Información propuesto para la empresa Telemarketing S.A.S abarca los procesos y subprocesos correspondientes al Departamento de Tecnología, incluyendo además a los actores que intervienen en el tratamiento de información con el fin de cumplir la normativa vigente en materia de protección de datos y de la norma ISO\IEC 27001:2013.

Dentro del alcance se contempla las instalaciones físicas de la organización (en todas sus sedes) que alojen activos informáticos, es decir, los centros de datos, pero también los lugares donde se almacenen datos y donde se opere con este tipo de dispositivos, de tal forma que sean protegidos y usados correctamente.

Se agrega al alcance la gestión de los activos informáticos, es decir su uso, almacenamiento y transporte (dentro y fuera de la organización), así como los medios por medio de los cuales se realizando dichas actividades, como son equipos de comunicaciones, redes de voz y datos, equipos de procesamiento y alojamiento (servidores) y equipos de usuario final (computadores, teléfonos móviles, tabletas, entre otros).

Otras áreas de la organización son excluidas, excepto en los casos puntuales que realicen gestión de información y/o activos informáticos. Físicamente se excluyen áreas o zonas que no tienen relación o influencia con el procesamiento y/o almacenamiento de datos o archivos.

12.2 POLÍTICA GENERAL

La información es un activo valioso para la operación de la organización Telemarketing S.A.S, considerando que es tanto el insumo principal para sus actividades como el producto final de las mismas y por tal razón existe un compromiso para con sus clientes, con sus proveedores, con las entidades de control y para consigo misma para protegerla y minimizar los riesgos a los cuales está expuesta partiendo desde una de las principales áreas de soporte y apoyo: El Departamento de Tecnología.

En este esfuerzo de cumplir con los lineamientos que se desprenden de la implementación del Sistema de Gestión Telemarketing S.A.S se compromete, entre otras cosas, a:

- Impulsar una cultura de seguridad de la información en sus empleados y personal externo a través de la formación y la capacitación y del cumplimiento de los procesos y políticas que de este sistema se desprendan.

- Gestión oportuna de los incidentes de seguridad, de la continuidad del negocio y de los procesos para la seguridad de la información.

- Mantener un proceso continuo de mejora del Sistema de Gestión de Seguridad de la Información que incluye la revisión del sistema, mantenerlo vigente, actualizado y acorde a la operación de la organización.

- Realizar la gestión de los activos de información y aplicación de los niveles adecuados de protección.

- Mantener y promover una estructura dentro de la organización, llamado Comité de Seguridad, que sostenga el Sistema de Gestión de Seguridad de la Información y

valide el cumplimiento de las políticas, procesos y controles que desde allí se generan.

La Política de la Seguridad de la Información a su vez cumple con los siguientes requisitos:

- La política de seguridad de la información es aprobada y publicada por la dirección de la organización.
- Es accesible a todo el personal de Telemarketing S.A.S y a personal externo vinculado a la organización.
- El Comité de Seguridad de Telemarketing S.A.S es el propietario de la Política y responsable de su mantenimiento, revisión, desarrollo y cumplimiento.
- La Política de Seguridad de la Información tendrá en cuenta y será acorde con las revisiones realizadas por Telemarketing S.A.S a otras áreas que puedan generar nuevos requerimientos, modificaciones y mejoras.
- La Política de Seguridad de la información afecta a todo el personal interno y externo, los sistemas de información y las ubicaciones físicas relacionadas con dichos sistemas.

Por último, se definen los objetivos de la seguridad de la información:

- Dirigir y dar soporte a la gestión de la seguridad de la información acorde con los requisitos del negocio, la legislación y las regulaciones aplicables.
- Proteger la información y minimizar los riesgos a los que está expuesta.

12.3 POLITICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

12.3.1 Organización para la seguridad de la información

Objetivo: Definir la estructura dentro de la organización responsable del SGSI, su implementación y mantención.

Sanciones: El personal designado estará sujeto a las sanciones disciplinarias que apliquen al incumplimiento de funciones, según lo dispuesto por el departamento de Gestión de Talento Humano y bajo las normas laborales vigentes.

Telemarketing S.A.S establecerá una estructura en la organización encargada de la implementación y gestión del Sistema de Gestión de Seguridad de la Información, así como de los procesos de formación y capacitación, y de la asignación de los recursos necesarios para el buen funcionamiento del sistema.

La estructura dentro de la organización deberá tener en cuenta los siguientes aspectos y actividades a realizar por Telemarketing S.A.S:

- Redactar las funciones y responsabilidades de obligado cumplimiento por parte del personal interno y externo de la organización, con especial énfasis en las regulaciones y normas. Documento “Funciones y Responsabilidades”.

- Definir, evaluar y establecer los criterios para autorizar e incorporar nuevos recursos a los sistemas de información. Documento “Procedimiento de autorización de recursos”.

- Definir, evaluar y establecer las condiciones necesarias para mantener la confidencialidad de la información entre los empleados de la organización y externos que usen información confidencial, mediante las cláusulas y políticas correspondientes. Documento: “Cláusula de Confidencialidad”.

- Definir, mantener y actualizar el directorio de contactos de emergencia a cargo del Responsable de Seguridad de la Información y las áreas técnicas relacionadas con el SGSI. Documento: “Directorio de Contactos de Emergencia”.

- Desarrollar el contacto con los miembros de la organización y miembros de otras organizaciones para la gestión de incidentes de seguridad de la información, continuidad del negocio y planes de contingencia.

- Desarrollar el contacto con las autoridades relacionadas con la legislación, regulación y normatividad relacionada con la seguridad de la información, así como con los proveedores de servicios.

- Desarrollar un proceso de actualización y capacitación del área técnica en relación con la seguridad de la información, así como el contacto con medios informativos especializados en el área.

- Desarrollar y ejecutar un cronograma de auditorías independientes para el Sistema de Gestión de Seguridad de la Información.

12.3.1.1 Responsables de la seguridad de la información

Objetivo: Determinar los responsables directos en la implantación del SGSI, la ejecución de las políticas y su mejora en el tiempo.

Sanciones: El personal designado estará sujeto a las sanciones disciplinarias que apliquen al incumplimiento de funciones, según lo dispuesto por el departamento de Gestión de Talento Humano y bajo las normas laborales vigentes.

Telemarketing S.A.S designa la responsabilidad de la gestión del Sistema de Gestión de Seguridad de la Información en el responsable del Departamento de Tecnología de la Organización, quién cumple con las siguientes funciones (y aquellas adicionales que el Comité de Seguridad asigne en función de nuevos requerimientos):

- Velar por el mantenimiento, desarrollo y aplicación del Sistema de Gestión de Seguridad de la Información.

- Aplicar, verificar y gestionar las actualizaciones\cambios de los procedimientos, políticas y controles establecidos en el SGSI.

- Definir periódicamente y velar por la ejecución de los programas de mantenimiento de los activos.

- Implantar, administrar y gestionar los sistemas informáticos dentro de la organización de forma segura, o direccionar a los usuarios para el uso adecuado de los mismos.

- Proponer, coordinar y aplicar los cambios necesarios en el sistema de información acorde con los requerimientos de la organización y los lineamientos del SGSI.

- Controlar los procedimientos de generación de respaldos de información y pruebas de restauración de estos.

- Gestionar y velar por el uso de software licenciad y el respeto a las leyes de protección de datos personales y derechos de autor.

Adicionalmente, la labor administrativa del responsable del Departamento de Tecnología\Responsable del Sistema de Gestión de Seguridad de la Información será apoyada a nivel operativo por el equipo de soporte de tecnología de la organización, quienes tendrán las siguientes responsabilidades:

- Mantener, soportar y gestionar el sistema de información de la organización.
- Administrar los usuarios y contraseñas, incluida alta, baja y suspensión de los usuarios de la organización en el sistema de gestión de usuarios.
- Aplicar los controles y políticas para la protección y gestión de los sistemas operativos y otros softwares usados por la organización.
- Aplicar los controles y políticas de seguridad para la protección y gestión para el uso seguro de los recursos web en la organización.
- Aplicar los controles y políticas de seguridad para la protección y gestión para el uso seguro de los recursos de hardware en la organización.
- Ejecutar los procedimientos de copias de seguridad de la información y realizar las pruebas de restauración.
- Ejecutar el cronograma de mantenimiento preventivo y correctivo de los dispositivos (Hardware) de la organización, así como aplicar las medidas de mejora\adaptación.
- Cumplir con el registro de las actividades, incidentes, o cualquier otra información de acuerdo con los lineamientos del SGSI.

12.3.1.2 Contactos con las autoridades

Objetivo: Mantener un listado de las autoridades y organizaciones relacionadas con la seguridad de la información.

Responsable: Departamento de TI – Departamento de Gestión de Talento Humano.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones (Ej. llamado de atención).

El Departamento de Tecnología, en conjunto con el Comité de Seguridad, el director de la Telemarketing S.A.S y las áreas que componen el soporte de la organización gestionan y actualizan el directorio de contactos con las siguientes organizaciones consideradas fundamentales en la gestión de la seguridad (tanto a nivel de información, así como de infraestructura y humana):

- Departamento de Policía.
- Departamento de Bomberos.
- Defensa Civil.
- Oficina de Ciberseguridad de la Policía Nacional de Colombia.
    - Equipo de respuesta a incidentes de seguridad informática.
- Grupo de Informática Forense Cuerpo Técnico de Investigación (Fiscalía).
- Grupo de Informática Forense Policía Judicial.
- COLCERT – MINDEFENSA Grupo de respuesta a emergencias cibernéticas de Colombia.

Adicionalmente el Departamento de TI mantendrá contacto o se actualizará con la información de las entidades que sobre seguridad informática se encuentran en Colombia, por ejemplo:

- CSI Colombia – Consultores de Sistemas de Información.
- Grupo Atlas de Seguridad.
- ASTAF - División de tecnologías de la información y las comunicaciones.
- Hack & Secure.
- Information Security Systems.
- IT Forensic.
- Foros y grupos de ingeniería especializados.

12.3.2 Personal externo

Objetivo: Determinar la forma de relacionar con el personal externo, forma de contratación y cláusulas a incluir.

Responsable: Gestión de Talento Humano y Departamento de IT.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones (Ej. llamado de atención). Adicionalmente la suspensión del contrato de acuerdo con gravedad o nivel de incumplimiento.

En relación con el personal externo, Telemarketing S.A.S tendrá en cuenta los siguientes criterios:

- Disponer de un documento informativo sobre las políticas de seguridad de la información de Telemarketing S.A.S que será entregado al personal externo que se vincule con la empresa.

- Establecer el procedimiento de selección y vinculación de personal-entidades externas para operar con Telemarketing S.A.S, adecuando el(los) contrato(s) de acuerdo con las funciones\labores que dicho externo realizará.

- Disponer del documento “Acuerdo de Confidencialidad” para externos que se vinculen con Telemarketing S.A.S que debe ser gestionado y firmado por dicho personal. Los acuerdos de confidencialidad con externos deberán ser revisados periódicamente por el Responsable de Seguridad.

- Disponer de un documento\registro donde figuren, entre otros:

    - Tercero.
    - Fecha de Vinculación.
    - Activo(s) al (a los) cual(es) tiene acceso.
    - Motivo del acceso.
    - Tipo de acceso.
    - Fecha caducidad del acceso.
    - Persona que autoriza el acceso.

12.3.3 Gestión de activos

La sección gestión de activos está enfocada en la protección y uso y almacenamiento adecuado de los activos informáticos de la organización.

12.3.3.1 Inventario de activos de información

Objetivo: Mantener el control sobre los activos de información de la organización.

Responsable: Departamento de TI.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones (Ej. llamado de atención).

El departamento de TI de la Telemarketing S.A.S deberá llevar un control de los activos de información, considerando:

- Se debe llevar registro de todos los activos informáticos, sus características, ubicación, propietario, fecha de ingreso y fecha de baja.
- Se debe realizar un inventario periódico, no mayor a 6 meses, donde se constate la validez y/o veracidad de la información registrada.
- Se debe realizar actualización del inventario cada vez que se realicen ingresos o salidas (bajas de activos) o modificaciones a los mismos.

Adicionalmente se recomienda realizar un procedimiento para la disposición final de los Residuos de Aparatos Eléctricos y Electrónicos (**RAEE**) a través de una empresa certificada en el manejo de dichos elementos.

12.3.3.2 Uso de la información

Objetivo: Definir y asegurar que la información recibe un nivel adecuada de protección.

Responsable: Departamento de TI en cuanto a la definición del uso, toda la organización en cuanto al uso de la información.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones (Ej. llamado de atención).

Para asegurar el correcto uso de la información dentro de la organización mediante una correcta gestión y control de los activos. Con este fin se definen los siguientes requisitos:

- Telemarketing S.A.S dispone del inventario de los activos de información debidamente identificados. El Responsable de Seguridad de la Información vela por mantener el inventario debidamente actualizado y gestionado.
- Dispondrá del registro que relaciona el activo de información junto con el propietario y/o usuario de este.
- La responsabilidad del activo recae sobre el propietario\usuario de este, quien debe asegurarse que esté debidamente identificado y asegurado.
- Dispondrá del documento “Norma de uso de la información y activos de la información” que será de conocimiento de todos los miembros internos de la organización y los externos para su debido cumplimiento.

12.3.3.3 Clasificación de la información

Objetivo: Definir y clasificar la información y su relevancia para la organización, así como la manera en que será tratada.

Responsable: Departamento de TI en cuanto a la asignación de los niveles de clasificación; toda la organización en cuanto al cumplimiento de la clasificación.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con nivel de clasificación de la información, siendo la sanción directamente proporcional al nivel de información (la información confidencial debe ser preservada y conlleva sanciones drásticas ante su difusión o manipulación no autorizada).

Telemarketing S.A.S implementará un sistema de clasificación de la información que permita identificar la importancia del activo dentro del sistema:

- La información gestionada y almacenada dentro de las instalaciones, equipos y soportes de Telemarketing S.A.S es propiedad de la empresa y no de los

usuarios\externos, a excepción de la información incluida en la ley de protección de datos personales.

- La información será clasificada para que sea protegida debidamente según su nivel de importancia en el sistema, su valor, la relación con los usuarios o requerimientos legales. Los activos que soporten de información serán evaluados según la información que contengan.

- Se usarán los siguientes niveles en la clasificación de la información:

    - Información Confidencial: Se clasificará como confidencial toda aquella información que se considere no puede ser revelada excepto bajo criterios específicos, justificados y autorizado del propietario de esta, cuya pérdida, modificación o indisponibilidad genere un riesgo no aceptable para la organización o que bajo la normatividad vigente deba ser clasificada de esa forma.

    - Información de uso interno (restringida): Se clasificará como información de uso interno aquella que, al ser revelada, pérdida, modificada o estar inaccesible genera un riesgo aceptable para la organización.

    - Información pública: Toda información cuya divulgación, pérdida o modificación no genere un riesgo a la organización ni infrinja ninguna ley, especialmente aquellas relacionadas con protección de datos personales.

- Los activos de información podrán cambiar su clasificación de CONFIDENCIAL a USO INTERNO a solicitud del propietario y con la autorización del Responsable de Seguridad de la Información.

12.3.3.4 Etiquetado de la información

Objetivo: Implementar una señalización visual que permita identificar la clasificación de la información.

Responsable: Propietario de la información.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación al incumplimiento de funciones asignadas.

El proceso de etiquetado debe aplicarse a la información y a los activos que la contengan considerando la clasificación de esta y los siguientes criterios:

- Todo activo de información (datos o contenedores) propiedad de la organización y que no se encuentre etiquetado será considerado como información pública.

- Todo activo de información (datos o contenedores) propiedad de la organización y que disponga de la imagen corporativa de Telemarketing. S.A.S se clasifica automáticamente como información de “USO INTERNO” y no requiere etiqueta explicita. En caso de llevar etiqueta debe estar incluida en la portada, se sugiere aplicarla en otros espacios como los pies de página.

- Los activos de información en soporte electrónico, propiedad de Telemarketing S.A.S o generados allí, son considerados como de “USO INTERNO” y no requiere etiqueta explicita. En caso de llevar etiqueta debe ir ubicada sobre la superficie del soporte.

- Todo activo de información (datos o contenedores) cuya clasificación sea información pública será etiquetado con la etiqueta “USO PÚBLICO”.

- Todo activo de información (datos o contenedores) cuya clasificación sea de información confidencial deberá llevar la etiqueta “CONFIDENCIAL”:

    - Soporte en papel: deberá llevar la etiqueta “CONFIDENCIAL” en cada hoja que haga parte del documento, incluida la portada.

    - Soporte electrónico: deberá llevar la etiqueta “CONFIDENCIAL” en la superficie del soporte.

12.3.3.5 Cifrado de la información

Objetivo: Implementar mecanismos de seguridad en la transmisión de la información

Responsable: Propietario de la información.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones asignadas.

La información que se almacena o se transmite a través de medios electrónicos, en especial aquella catalogada como confidencial o de uso interno deberá ser protegida

mediante mecanismos de cifrado seleccionados y autorizados por el Departamento de TI.

12.3.3.6 Firma Electrónica

Objetivo: Implementar un mecanismo para garantizar la autenticidad de la información.

Responsable: Propietario de la información.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones asignadas.

Telemarketing S.A.S proveerá a los propietarios de la información, a través del Departamento de TI, de los mecanismos de firma electrónica autorizados que permitan garantizar la identificación del propietario y la autenticidad de los documentos. El proceso de firma electrónica deberá ser aplicado a:

- Documentos de tipo confidencial.
- Documentos de uso restringido.
- Documentos de carácter legal.
- Documentos entregados a entes reguladores.
- Cualquier otro documento considerado por parte del Comité de seguridad o solicitado por un ente externo.

Para la implementación de firma electrónica se debe considerar:

- Debe ser un mecanismo conocido y certificado por una organización especializada en este tipo de elementos.

- Debe ser un mecanismo autorizado por las organizaciones reguladoras con las cuales tiene relación Telemarketing S.A.S.

- En lo posible debe ser un mecanismo de fácil uso/aplicación por parte de los propietarios de la información.

- El mecanismo seleccionado no debe entrar en conflicto con otros sistemas de firma electrónica exigidos de forma específica por entidades de orden gubernamental o fiscal.

- Se debe llevar un registro de las firmas electrónicas asignadas, especificando el usuario, fecha de entrega, características de la firma, respaldo, entre otros.

12.3.4 Medios removibles

Objetivo: Asegurar el uso correcto y seguro de medios extraíbles.

Responsable: Departamento de TI.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones asignadas.

El uso de medios removibles (CD, DVD'S, Memorias USB, Discos Duros Externos, entre otros similares) estarán sujetos a las siguientes condiciones:

a. Se aplicará por defecto la política de denegación de acceso a medios removibles externos para toda la organización.

b. Solo se habilitará el uso de medios removibles a personal de estructura y administrativo con la autorización del Responsable de Seguridad de la Información y/o el Comité de seguridad.

c. Los puestos de operación solo podrán tener habilitado el uso de medios removibles en los casos que la falta de los mismo impida la ejecución normal de las actividades de los agentes, coordinadores, supervisores y jefes de proyectos. Debe contarse con la autorización y conocimiento justificado del Responsable de Seguridad de la Información y el Comité de Seguridad, además debe estar documentado.

d. Las áreas o empleados que hagan uso de medios removibles deben tener en cuenta:

    a. Los funcionarios serán directamente responsables de los medios y de la información allí contenida.

    b. Los funcionarios deben asegurar física y lógicamente el medio y la información que contiene con el fin de no comprometer la disponibilidad, integridad y confidencialidad de la información.

e. El retiro de medios extraíbles de las instalaciones de la organización estará controlado y debidamente registrado, incluido el contenido que portan. Los medios estarán debidamente encriptados.

12.3.5 Respaldo y copias de seguridad

Objetivo: Asegurar la protección de la información mediante copias de respaldo y la seguridad de los medios que almacenan dichas copias.

Responsable: Departamento de TI.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones asignadas.

El Departamento de TI de Telemarketing S.A.S realizará los procesos respectivos para la generación de copias de respaldo de la información que se considere crítica para la operación de la empresa asegurando su disponibilidad, integridad:

- Se realizarán copias de seguridad de la información crítica de la organización, incluidas:
    - Bases de datos operativas.
    - Bases de datos administrativas.
    - Bases de datos financieras.
- Se definiría la periodicidad de las copias de seguridad de acuerdo con el nivel de criticidad de la información pudiendo ser diaria pero no mayor a un mes.
- Las copias de seguridad diarias podrán ser incrementales siempre que exista una copia de seguridad completa que cumpla con la frecuencia definida en el punto anterior.
- Las copias de seguridad deberán ser almacenadas en lugares seguros, fuera del alcance de personas no autorizadas y de riesgos de tipo ambiente y/o industrial. En lo posible deberán ser administradas\gestionadas por un software especializado en estas tareas.

- Los medios físicos donde se almacenan las copias de seguridad deberán contemplar la posibilidad de ubicarse en instalaciones físicas diferentes a las de la misma empresa.

- En la gestión de las copias de seguridad se debe incluir pruebas periódicas de las *backups* generados, por ejemplo, realizando test de importación. Estas pruebas no pueden ser superiores a un mes.

- Se debe llevar registro de:

    - Proceso de generación de copias de seguridad.
    - Proceso de pruebas de copias de seguridad.
    - Registro de almacenamiento de medios físicos con copias de seguridad.
    - Listado de fuentes de información incluidos en las copias de seguridad.

12.3.6 Recursos humanos

La sección de recursos humanos se enfoca en el aseguramiento que el personal interno y externo de la organización conoce y aplica las políticas de seguridad de la información establecidas por Telemarketing S.A.S.

12.3.6.1 Selección del personal

Objetivo: Asegurar que la selección de empleados internos y externos cumplen con los requisitos de seguridad de la información.

Responsable: Departamento de Gestión de Talento Humano.

Sanciones: Anulación de la contratación.

El proceso de selección de personal estará documentado por el Departamento de RRHH de Telemarketing S.A.S, considerando los siguientes criterios y políticas relacionados con la seguridad de la información:

- Se debe tener con un procedimiento de comprobación de los antecedentes de los futuros empleados y personal externo a vincular con la organización.

- Se debe legalizar la vinculación mediante contrato laboral que tenga incluido, entre otras cosas, lo siguiente:

- Funciones del empleado.
- Obligaciones por desempeñar.
- Procedimiento disciplinario aplicable.
- Proceso por seguir en caso de finalización de vínculo laboral.

- Telemarketing S.A.S debe mantener el soporte del a celebración del contrato o vínculo laboral, la aceptación de las responsabilidades y obligaciones, y cualquier otro soporte relacionado con el proceso de selección.

- Se debe tener documentado y definidos los perfiles asociados a cada cargo dentro de la organización, en los cuales se debe incluir:

    - Educación mínima exigida.
    - Experiencia laboral mínima exigida.
    - Formación mínima exigida.
    - Equivalentes a los ítems anteriores.

- El departamento de RRHH debe contar con el manual de funciones del empleado, que incluya las funciones y responsabilidades en el uso seguridad de la información.

12.3.6.2 Acuerdos de confidencialidad

Objetivo: Asegurar la implementación de acuerdos de confidencialidad en los contratos con empleados internos y externos y proveedores.

Responsable: Departamento de Gestión de Talento Humano, Departamento de Compras\Financiero.

Sanciones: Anulación del contrato.

El departamento de Gestión de Talento Humano se encargará de la redacción de los contratos de personal interno y externo; por su parte el departamento de Compras y/o financiero realizará lo respectivo a contratación con proveedores. En ambos casos se debe considerar lo siguiente:

- Determinar las funciones y obligaciones a desempeñar por el empleado, o las funciones y actividades para las cuales fue contratado el proveedor.

- Determinar cuáles son las actividades que involucran el tratamiento o manipulación de datos de carácter personal o los soportes que los almacenan o procesan.
- Deber de secreto en el tratamiento de datos de carácter personal o de los activos que los almacenan o procesan.
- Procedimiento disciplinario aplicable a los empleados.

12.3.6.3 Procesos disciplinarios

Objetivo: Definir los procesos disciplinarios antes las faltas a las políticas de seguridad de la información.

Responsable: Departamento de Gestión del Talento Humano.

Sanciones: No aplica.

Telemarketing S.A.S contará con un procedimiento redactado y documentado de procedimiento disciplinario que abarque las infracciones relacionadas a la seguridad de la información.

El procedimiento deberá ser de conocimiento del empleado en el momento de contratación y deberá quedar registro de su entrega y aceptación.

12.3.6.4 Desvinculación de empleados y cambio de puesto

Objetivo: Definir los procedimientos relacionados con la desvinculación de empleados y el cambio de puesto de trabajo.

Responsable: Departamento de Gestión del Talento Humano.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones asignadas.

Telemarketing S.A.S contará con un procedimiento redactado y documentado para el cambio de puesto que deberá tener en cuenta los siguientes criterios:

- Debe incluir un mecanismo de comunicación por parte de RRHH (o el área designada) al Responsable de Seguridad de la Información o su equipo de soporte, en el cual se comunique el(los) cambio(s) que se realizan en un plazo menor a 24 horas.

- El Responsable de Seguridad de la Información o su equipo de soporte retirará los permisos que están asociados al cargo actual y que no son requeridos en el nuevo puesto.

- El Responsable de Seguridad de la Información o su equipo de soporte asignará los permisos que están asociados al nuevo cargo y son requeridos para el desarrollo normal de sus funciones y no se encuentran previamente asignados al empleado.

- El Responsable de Seguridad de la Información o su equipo de soporte modificará los permisos para el acceso físico de acuerdo con los requerimientos del cargo.

- El Responsable de Seguridad de la Información o su equipo de soporte retirará o asignará los recursos informáticos (PC, laptop, móviles, entre otros) según los requerimientos del cargo. En todo caso deberá quedar documentado mediante acta la entrega o devolución de los activos en el que conste el estado en que se encuentran, accesorios, recomendaciones, entre otros.

Telemarketing S.A.S contará con un procedimiento redactado y documentado para el cese o desvinculación de empleados que deberá tener en cuenta los siguientes criterios:

- Debe incluir un mecanismo de comunicación por parte de RRHH (o el área designada) al Responsable de Seguridad de la Información o su equipo de soporte, en el cual se comunique el(los) ceses(s) o desvinculación(es) que se realizan en un plazo menor a 24 horas.

- El Responsable de Seguridad de la Información o su equipo de soporte procederá a la inhabilitación de los usuarios y los permisos asociados al cargo\empleado.

    - Se deberá considerar los tiempos mínimos requeridos por la organización o la legislación vigente relacionado con la información histórica del empleado en el sistema.

- El Responsable de Seguridad de la Información o su equipo de soporte retirará o los recursos informáticos (PC, laptop, móviles, entre otros) según los requerimientos del cargo. En todo caso deberá quedar documentado mediante

acta la entrega o devolución de los activos en el que conste el estado en que se encuentran, accesorios, observaciones, entre otros.

- El Responsable de Seguridad de la Información o su equipo de soporte retirará los permisos de acceso físico a las instalaciones de la organización. Se deberá considerar, de acuerdo con los requerimientos de la organización o de la legislación vigente, mantener los registros históricos del empleado en la organización.

12.3.7 Control de acceso

La sección 8.4 hace referencia al control que se realiza al acceso a la información, los recursos informáticos (tanto almacenamiento como procesamiento) y los procesos que se realizan con o sobre dichos recursos. Este control debe estar documentado o incluido en los procedimientos, y definido por la organización e implementados.

12.3.7.1 Gestión de control de acceso lógico

Objetivo: Controlar el acceso a la información y los activos que los soportan y procesan.

Responsables: Toda la organización.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones asignadas.

El acceso lógico debe ser controlado mediante el uso de elementos que identifiquen unívocamente a cada usuario y de igual forma debidamente autorizados por el propietario del recurso, por el Responsable de Seguridad de la Información o por el Comité de Seguridad. El acceso al recurso debe quedar registrado.

Para la gestión del control de acceso lógico se deberán considerar los siguientes elementos:

- Niveles de acceso.
    - Nivel 1 – Acceso a los servicios de red: Considera los accesos a:
        - Redes de comunicaciones y filtrado de conexiones.

        - Protocolos de red autorizados.
        - Usos permitidos en entornos de red (Correo, internet, DNS, entre otros).

    - Nivel 2 – Acceso a dominio ofimático: Incluye lo siguiente:

        - Entorno ofimático y uso de recursos compartidos.
        - Acceso mediante identificación y autenticación en Directorio Activo o LDAP.

    - Nivel 3 – Acceso a datos: Contiene:

        - Acceso a la información respecto a funciones y responsabilidades.
        - Acceso a la información para la ejecución de las actividades de la organización.
        - Acceso a las aplicaciones y gestores de bases de datos.

- Permisos de acceso: En la asignación de los permisos de acceso se deben considerar los siguientes criterios:

    - Se aplicará como política general la denegación total.

    - Se habilitará el acceso a lo explícitamente definido o permitido.

    - Todos los usuarios accederán mediante la combinación de identificador y contraseña.

    - LA responsabilidad sobre el identificador y la contraseña, así como el uso que se haga de dicho elementos y exclusiva del usuario al que se le han asignado.

    - Todas las actividades realizadas con los usuarios que cuenten con rol administrativo deberán ser registradas para su consulta y auditoría.

    - Los usuarios tendrán acceso autorizado únicamente a la información y los recursos necesarios para sus funciones y cualquier acceso no autorizado quedará registrado.

    - El sistema se configura para permitir como máximo 3 intentos de acceso fallido a la información o al recurso, posterior a esto se bloqueará el identificador de usuario.

    - El acceso a los espacios físico donde se encuentre el soporte informático estará restringido y controlado mediante un sistema de control físico que impida el acceso a personal no autorizado.

- El nivel de acceso y los privilegios de cada usuario (o tipo de usuario) deberán estar documentados.

- El acceso a información o recursos de nivel alto (ejem: confidenciales) deberá estar registrado, con por lo menos la siguiente información:

    - Identificación del usuario.
    - Fecha y hora del acceso.
    - Tipo de acceso.
    - Autorización (responsable de autorizar el acceso).

- Solo el Responsable de Seguridad de la Información y el equipo de soporte están autorizados para conceder, alterar, retirar los accesos sobre la información o recursos.

- Toda la información relacionada con los usuarios, identificadores, contraseñas, registros, entre otros, deberá cumplir con las normativas de protección de datos personales vigentes.

12.3.7.2 Gestión de usuarios

Objetivo: Definir las pautas para la gestión de usuarios.

Responsable: Departamento de Gestión de Talento Humano y Departamento de TI.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones asignadas.

Para la gestión de usuarios en la organización se deben tener los siguientes criterios:

- Se deberá contar con un procedimiento para el alta, modificación y baja de usuarios.

- El responsable de seguridad de la información o el equipo de soporte será el encargado de asignar el identificador, la contraseña y los accesos a los usuarios.

- Cada usuario\empleado de la organización deberá contar con su respectivo identificado y contraseña, desde el mismo momento en que ingresa o se da de alta en la organización.

- La combinación de identificador y contraseña es personal e intransferible, siendo el usuario completamente responsable de las consecuencias que se generen por su mal uso, pérdida o divulgación.

- La combinación de identificador y contraseña será inhabilitada inmediatamente se informe la baja del usuario\empleado en la organización.

- Toda acción realizada con el identificador sobre información o recursos considerados como susceptibles para la organización deberá quedar registrado.

- El responsable de cada área revisará con una frecuencia no mayor a 6 meses el listado de usuarios de las aplicaciones corporativas pertenecientes a su unidad y comunicará al Responsable de Seguridad los cambios necesarios.

En la asignación del identificador del usuario se deberá considerar un estándar que permita identificarlo incluyendo lo siguiente:

- Se deberá generar un identificador único para cada usuario.

- Deberá identificar el área al que pertenece el usuario (ejemplo: “adm” para administración, “tec” para tecnología, entre otros).

- Identificar la sede de la organización (Ejemplo: “01” para Colombia, “PER” para Perú, entre otros).

- Identificador relacionado con los nombres del usuario, pudiendo ser parte del nombre y del apellido, combinación de nombre y apellido, entre otras.

- Deberá incluirse un elemento para evitar coincidencia (ejemplo un número, inicial de segundo apellido, entre otros).

- Se deberá contar con un procedimiento de creación de identificador en el cual se defina las reglas o parámetros que se seguirán para esta tarea.

En relación con el personal de TI se debe considerar lo siguiente:

- Los miembros del Departamento de TI son las únicas personas autorizadas para usar múltiples cuentas y deberán contar con al menos dos tipos:

    - Usuario sin privilegios o usuario estándar, para las funciones normales dentro de la organización.
    - Usuario con privilegios o administrador, para el cumplimiento de funciones o tareas relacionadas con administración y/o gestión de los sistemas a alto nivel.

  Los usuarios de TI usarán principalmente los usuarios estándar o sin privilegios para sus labores normales limitando el uso de las cuentas de administración solo para actividades específicas y, en lo posible, por tiempos limitados.

- Los usuarios de TI con tareas de auditoría deberán contar con cuentas específicas (adicionales) para tareas de auditoria.

- Los usuarios de TI con tareas de administración de seguridad deberán contar con cuentas específicas (adicionales) para este tipo de actividades.

12.3.7.3 Gestión de contraseñas

Objetivo: Asegurar la correcta creación, uso y protección de las contraseñas.

Responsable: Departamento de TI en la gestión técnica de las contraseñas; toda la organización en el uso y protección de las contraseñas.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones asignadas. Los usuarios deberán asumir la responsabilidad y sanciones derivadas del uso de sus credenciales de acceso cuando se confirma que no se han cumplido con las políticas de seguridad.

La gestión de contraseña deberá considerar los siguientes aspectos:

- Las contraseñas son confidenciales.

- Las contraseñas deberán cumplir con las siguientes características:

    - Deben tener una longitud mínima de 8 caracteres alfanuméricos.
    - Deben tener mínimo una letra mayúscula, mínimo una letra minúscula y un carácter numérico.

- Debe contener al menos un carácter especial (punto, asterisco, etcétera).
- No debe tener el nombre o apellido del usuario.
- No debe tener secuencias alfanuméricas (“123456”, “abcdefg”, entre otros).
- No se permite más de dos caracteres seguidos repetidos (“aaaaa”, “bbbbb”, “00000”).

- Al momento de asignar la contraseña esta debe ser temporal y deberá ser cambiada por el usuario en el primer ingreso al sistema.

- Las contraseñas deberán ser cambiadas por el usuario al menos cada seis meses.

- Las contraseñas no deben ser compartidas con otros usuarios y no deben ser almacenadas en medios físicos susceptibles de ser perdidos o hurtados.

12.3.8 Criptografía

El objetivo de los controles criptográficos es el de proteger la confidencialidad, la autenticidad o la integridad de la información.

12.3.8.1 Gestión de cifrado de dispositivos

Objetivo: Establecer las condiciones para el cifrado de dispositivos como medio de protección a la información que allí se contiene.

Responsables: El Departamento de TI en la implementación de los mecanismos en los dispositivos.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones asignadas.

Telemarketing S.A.S. implementará el cifrado de dispositivos considerando lo siguiente:

- Los mecanismos de cifrado seleccionados deberán considerar la protección de la información a nivel de:

    - Confidencialidad: Protección de la información cuando es transmitida por diferentes medios.

- Integridad\autenticidad: Uso de firmas digitales para proteger la autenticidad de la información.

- No repudio: técnicas criptográficas para obtener pruebas de la existencia o inexistencia de un evento o acción.

- Definir una política de encriptación que considere entre otras cosas:

  - Contingencia ante la pérdida de claves de cifrado.
  - Riesgo ante la imposibilidad de aplicar medidas de seguridad y revisión (Ej. Antivirus).

- Usar algoritmos de cifrado que cumplan con las siguientes condiciones:

  - Algoritmos con una longitud mínima de clave de 128 bits, preferentemente 3DES, IDEA, RC4, RC5, AES.
  - Usar protocolos de comunicación cifrados como SSL\TLS.
  - Usar protocolos de correo cifrados como S\MIME.
  - Usar protocolos de sesión remota como SSH.

- Aplicar cifrado de disco duro en dispositivos portátiles (computador portátil, teléfono móvil, entre otros).

- Aplicar cifrado en los medios extraíbles que contienen información confidencial o sensible (USB, CD ROM, entre otros).

- Utilizar sistemas, software o hardware, que cuente con funcionalidades de seguridad y cifrado reconocidas y certificados.

12.3.8.2 Gestión de claves criptográficas

Objetivo: Definir las políticas para preservación y protección de las claves criptográficas.

Responsable: Departamento de TI.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones asignadas.

En la gestión de claves criptográficas se deben considerar los siguientes aspectos:

- Proteger físicamente los dispositivos de generación, almacenamiento y archivo de claves.
- Proteger la confidencialidad de las claves.
- Proteger las claves ante la modificación o destrucción.
- Almacenar correctamente las claves y controlar el acceso de los usuarios a ellas.
- Implementar una política de actualización de claves.
- Definir un procedimiento ante la pérdida\robo de claves criptográficas.
- Definir un procedimiento de revocación de clave que incluya su anulación o desactivación.
- Disponer de un procedimiento de recuperación de claves en caso de pérdida o corrupción.
- Se debe contar con copias de seguridad de las claves criptográficas.
- Disponer de un procedimiento de destrucción de claves.
- Llevar un registro de las acciones realizadas sobre las claves.

12.3.9 Instalaciones y seguridad física

Las instalaciones físicas de la organización involucran una parte importante de la operatividad de la empresa, puesto que afectan a las personas que allí trabajan como a los activos informáticos que allí se encuentran. La seguridad física hace referencia a los espacios donde se encuentran o almacenan la información y los recursos asociados a esta, los cuales deben ser restringidos y protegidos adecuadamente con controles de acceso.

Ambos elementos, instalaciones y seguridad física, están relacionados y es importante que sean protegidos debidamente y hagan parte de los protocolos de seguridad del SGSI (siempre en el marco del alcance definido).

12.3.9.1 Inventario

Objetivo: Mantener un registro de los activos físicos correspondientes a las instalaciones de la organización.

Responsable: Departamento de TI.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones asignadas.

El departamento de TI de Telemarketing S.A.S llevará el inventario de las instalaciones físicas de la organización en apoyo con el área de mantenimiento general. El inventario cumplirá con las siguientes condiciones:

- Registro de las diferentes sedes que componen la organización.
- Registro de las diferentes zonas que componen cada zona.
- Categorización de las zonas (área pública, restringida, entre otras).

12.3.9.2 Perímetro de seguridad física

Objetivo: Prevenir los accesos no autorizados, daños e interferencias a las instalaciones físicas.

Responsable: Departamento de TI, Dirección de la organización.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones asignadas.

Telemarketing S.A.S define los espacios que corresponden al perímetro físico de la organización, considerando los recursos que se ubican en dichos lugares, señalizándolos adecuadamente y aplicando los controles pertinentes.

Para la definición y gestión del perímetro de seguridad física se debe considerar:

- Las áreas dentro de la organización deberán ser clasificadas de la siguiente forma:

    - Áreas públicas: Espacios sin restricción, accesibles a personal de la organización, externos, visitantes, entre otros.

    - Áreas internas: Espacios reservados para personal interno (empleados) y personal externo contratado por la organización. Los recursos informáticos en estos espacios serán de tipo público o nivel bajo.

    - Áreas de acceso restringido: Espacios con acceso reservado a un grupo específico de empleados y personal externo, autorizados por el Responsable de Seguridad de la Información o el Comité de Seguridad. Este espacio contiene recursos de información críticos para la organización.

- El perímetro del edificio o instalación debe ser físicamente sólido, equipos con puertas seguras y los accesos externos (puertas y ventanas) aseguradas ante accesos no autorizados.

- Se debe instalar sistemas de detección de intrusos conforme a las normas o legislación vigente, y estos deben ser probados periódicamente.

- Se debe realizar una revisión periódica de las instalaciones físicas y registrar el proceso para acciones de revisión y/o auditoría.

- El almacenamiento de materiales inflamables o peligrosos se realizará en espacios adecuados para tal fin y bajo condiciones adecuadas.

- Los equipos y los soportes de respaldo no se ubicarán en el mismo espacio físico que los equipos y soportes principales.

- Siempre que sea posible, se debe contar con un área pública separada de las áreas internas o restringidas. En la zona pública se realizará el control y la restricción de acceso a las otras zonas de la organización.

- Siempre que sea posible, se instalarán barreras físicas para controlar y evitar el acceso no autorizado de personas a las instalaciones físicas de la organización.

- La organización debe contar con la cobertura de una aseguradora de riesgos profesionales, pólizas de aseguramiento contra todo riesgo para empleados, instalaciones, riesgos a terceros, bienes y personal en caso de accidentes laborales.

- Es requisito para todos los empleados, personal externo y visitantes portar una identificación visible y, en caso de no llevarla, serán reportados con el área de seguridad con el fin de tomar las medidas respectivas.

12.3.9.3 Controles de seguridad para oficinas y otros espacios

Objetivo: Prevenir los accesos no autorizados, daños e interferencias a las instalaciones físicas.

Responsable: Departamento de TI, Dirección de la organización.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones asignadas.

- Se implementarán medios de identificación para los usuarios con el fin de prevenir el acceso no autorizado a zonas internas o restringidas.

- Los accesos a las zonas de carga y descarga deben estar restringidos solo a personal autorizado e identificado.

- Las zonas de carga y descarga deben estar acondicionadas para limitar el acceso de personal externo a zonas internas y restringidas.

- Las puertas de oficinas, zonas restringidas, zonas de área y descarga deberán permanecer cerradas durante los periodos de tiempo que no las zonas no sean usadas.

- En las áreas de acceso restringido se deberá contar con un listado o relación de personas (empleados y personal externo) con autorización de acceso permanente, el cual será revisado y actualizado periódicamente.

- El acceso a áreas restringidas deberá quedar registrado, indicando la persona que ingresa, fecha, hora y motivo.

- Todos los visitantes deben ser supervisados y acompañados por un empleado de la organización.

- El personal externo que deba realizar labores dentro de las instalaciones de la organización deberá estar acompañado o supervisado por personal interno.

- El acceso a los centros de procesamiento de datos debe ser controlado, supervisado y restringido únicamente al personal autorizado, manteniendo un registro de los accesos a dicha zona, especialmente cuando se trate de personal externo que debe realizar actividades en dicho espacio.

- Las zonas u oficinas que contengan información sensible o confidencias, equipos informáticos críticos, soportes informáticos o cualquier otro activo de alto nivel para la organización, deberán estar aseguradas mediante puertas con cerradura o accesos mediante tarjeta e incluir el uso de registro biométrico, especialmente en el ingreso a las instalaciones físicas de la empresa (acceso principal) y al centro de datos (será prioritario el acceso biométrico sobre otras modalidades).

12.3.9.4 Protección física contra desastres naturales, ataques maliciosos o accidentes

Objetivo: Prevenir incidentes relacionados con los desastres naturales, ataques maliciosos o accidentes en las instalaciones físicas de la organización.

Responsable: Departamento de TI, Dirección de la organización.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones asignadas.

- La ubicación física de la organización debe cumplir con las normativas de protección ante desastres y la legislación vigente.

- Las instalaciones físicas deben contar con sistema de protección contra incendios, y estas deberán ser revisadas periódicamente y registrar el proceso para acciones de revisión y/o auditoría.

- La organización deberá mantener y ejecutar un cronograma de mantenimiento de sus instalaciones con el fin de prevenir posibles incidentes relacionados con desastres naturales, ataques maliciosos o accidentes.

12.3.9.5 Trabajo en áreas seguras

Objetivo: Determinar las condiciones físicas y políticas que permitan asegurar el bueno funcionamiento y/o protección de los activos.

Responsable: Departamento de TI, Dirección de la organización.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones asignadas.

- Se deben establecer las condiciones ambientales básicas de temperatura, higiene, aislamiento eléctrico y sonoro y cualquier otra medida similar y/o complementaria tanto para los equipos (de acuerdo con los requerimientos técnicos) como para las personas.

- No se debe permitir el uso de equipos fotográficos o de video en zonas de acceso restringido, salvo autorización expresa del Comité de Seguridad o del Responsable de Seguridad de la Información.

12.3.10 Equipos informáticos

Los equipos informáticos, como soporte o como herramienta de procesamiento de datos, tienen importancia en el sistema de seguridad de la información, razón por la cual se deben tomar las medidas para evitar el robo, pérdida o uso no autorizado.

12.3.10.1 Seguridad y operación de los equipos informáticos

Objetivo: Garantizar la protección de los equipos que almacenan y/o procesan información, así como la disponibilidad de los servicios ofrecidos por estos.

Responsable: Departamento de TI en relación con equipos críticos (Servidores, Comunicaciones, entre otros) y toda la organización en cuanto a los equipos usados para dentro de la operación.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones asignadas.

En relación con los equipos, Telemarketing S.A.S considera los siguientes criterios:

- En relación con los centros de procesamiento de datos:

- Los servidores de aplicaciones, datos y sistemas de red se ubicarán en una zona segura con acceso restringido solo a personal autorizado.

- Los centros de procesamiento de datos deberán contar con sistemas de alimentación ininterrumpida y/o grupo electrógeno que garantice como mínimo el apagado controlado de los equipos.

- En relación con los equipos de operación:

    - Los equipos asignados al personal (administrativo y operación) solo serán instalados y administrados por personal de TI.

    - Ningún equipo que no sea propiedad de Telemarketing S.A.S podrá tener en su dispositivo de almacenamiento información confidencial de la organización.

    - Equipos, soportes de información y software solo podrán ser retirados de las instalaciones con la autorización del Responsable de Seguridad de la Información y deberá quedar registrado.

    - Los equipos no deben dejarse desatendidos, especialmente cuando se encuentren en lugares públicos o diferentes a las instalaciones físicas de la organización.

    - Los equipos destinados a operar fuera de las instalaciones, en caso de requerir tener información confidencial almacenada, deberá ser solo la estrictamente necesaria para sus funciones y deberá estar cifrada y asegurada mediante contraseña.

- En relación con las redes eléctricas y datos:

    - El cableado, eléctrico y de datos, deberá llevarse desde el cuarto eléctrico o centro de datos hasta los puntos finales a través de canales subterráneos u otros medios alternativos que permitan su protección (tubería certificada, canales no accesibles al público, cable blindado, entre otros).

    - Los armarios de cableado no deberán ubicarse en áreas públicas a menos que sea estrictamente necesario. En cualquier caso, los armarios deberán estar cerrados y asegurados con llave y las llaves deberán ser gestionadas por el personal de mantenimiento o por el departamento de TI.

    - El cableado eléctrico debe estar separado del correspondiente a datos y/o comunicaciones.

- El cableado, las conexiones y en general los armarios deben estar ordenados, marcados y en lo posible acompañados de diagramas y explicaciones para su manipulación y mantenimiento.

- Todos los fallos, errores o actividades realizadas en los equipos (incluidos mantenimientos preventivos y correctivos) deberán ser documentados y registrados.

12.3.10.2 Mantenimiento de los equipos

Objetivo: Garantizar el correcto funcionamiento de los equipos y el cronograma de mantenimiento.

Responsable: Departamento de TI.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones asignadas.

En relación con el mantenimiento de los equipos se deberá tener en cuenta lo siguiente:

- El departamento de TI se encargará de aplicar mantenimiento preventivo al parque informático de la organización (incluidos los equipos del centro de procesamiento de datos) con el objetivo de anticipar fallos en los sistemas.

- El mantenimiento de los ordenadores, servidores, equipos de comunicaciones (entre otros) será realizado únicamente por el departamento de soporte o por personal externo seleccionado y autorizado, siguiendo las especificaciones técnicas de los fabricantes.

- El departamento de IT deberá contar cronograma de mantenimiento preventivo de equipos, el cual deberá ser ejecutado y las actividades registradas.

- Para los equipos cuyo mantenimiento deba ser realizado por personal especializado.

12.3.10.3 Disposición final de equipos

Objetivo: Definir las acciones a realizar sobre los equipos o dispositivos que serán dados de baja de los activos informáticos.

Responsable: Departamento de TI.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones asignadas.

En relación con la disposición final de los equipos:

- Los equipos y dispositivos que contengan información confidencial deberán pasar por el siguiente proceso:
    - Eliminado lógico de la información de sus dispositivos de almacenamiento, preferentemente con software especializado en la tarea.
    - Destrucción física del dispositivo o equipo, preferentemente con el soporte de una empresa especializada en el manejo de Residuos de Aparatos Eléctricos y Electrónicos (RAEE).

12.3.11 Operaciones

La gestión de la operación y de los recursos es el objetivo de la sección de operaciones. Si bien la operación no es parte del alcance del SGSI, si es importante que se gestione y se documenten los procesos relacionados con TI, pero además que sean parte activa de los procesos de formación y capacitación de la organización.

12.3.11.1 Procedimientos documentados

Objetivo: Garantizar la correcta documentación de los procesos, específicamente los relacionados con el Departamento de TI y que puedan afectar la operación de la organización.

Responsable: Departamento de TI, Dirección de la organización.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones asignadas.

Los procedimientos relacionados con la operación, el procesamiento de información y la gestión de recursos deben ser documentados y deben estar disponibles. Entre ellos se destacan:

- Parada y arranque programado de sistemas y servicios.
- Parada y arranque no programado de sistemas y servicios.
- Reinicio de servicios.

Igualmente tener documentadas las actividades (Tareas y procedimientos) tanto el procedimiento como el registro:

- Actividades diarias:
    - Comprobaciones de entorno físico.
    - Generación y prueba de copias de seguridad.
    - Revisión de logs.
    - Supervisión de servidores.
    - Supervisión de redes.
- Actividades semanales:
    - Actualizaciones de seguridad.
    - Control de salas y equipamiento.
- Actividades mensuales:
    - Restauración de copias de seguridad.
    - Revisión de capacidad y estadísticas de equipos.
- Actividades Anuales:

- Revisión de plan de contingencia.
- Prueba recuperación ante desastres.
- Prueba de grupos electrógenos.

12.3.12 Gestion de cambios

Objetivo: Documentar y gestionar correctamente las solicitudes de cambios en la organización a nivel de TI.

Responsable: Departamento de TI, Dirección de la organización.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones asignadas.

Se dispondrá de un procedimiento de gestión de cambios de servicios de la información y/o procesamiento de información. El procedimiento debe contemplar:

- Criterios para la implantación de un nuevo sistema o la actualización de uno existente.
- Aspectos técnicos y de seguridad.
- Pruebas en entornos seguros.
- Implementación en la organización.

12.3.12.1 Gestión de ambientes

Objetivo: Garantizar la correcta gestión, crecimiento y capacidad de los recursos informáticos.

Responsable: Departamento de TI, Dirección de la organización.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones asignadas.

- Se debe contar con planificación de la gestión y crecimiento de los recursos en el corto y mediano plazo.
- Se debe contar con proyección de crecimiento en el tiempo.
- Se debe contar con una descripción del estatus actual de los sistemas informáticos.

12.3.12.2 Gestión de eventos

Objetivo: Llevar un registro y control de los eventos relacionados con la seguridad de la información que permita además su análisis y tratamiento respectivo.

Responsable: Departamento de TI.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones asignadas.

En la gestión de eventos se debe considerar lo siguiente:

- Se deben registrar todos los eventos relacionados con los sistemas de información que puedan comprometer la seguridad de la información.
- El registro de los eventos debe ser realizado de tal forma que cumpla con las siguientes condiciones:
    - Debe ser auditable.
    - Debe satisfacer los requisitos legales aplicables a eventos y trazas.
    - La información debe poder ser usada como evidencia digital en acciones jurídicas.
    - La configuración\sincronización de relojes (tiempo) debe ser correcta para que el registro sea fiel a las condiciones, fechas y horas en que se presenta.

- Debe tener un nivel de seguimiento-monitorización de acuerdo con las exigencias legales o lo definido por el responsable de seguridad en el análisis de riesgos.

- Debe incluir, al menos, la siguiente información:

  - Estado de los dispositivos de red (Rendimiento, estado y funcionamiento).

  - Versiones instaladas y cambios en los aplicativos.

  - Registro sobre el estado de la configuración y los cambios realizados.

  - Registros Syslog.

  - Revisión de los sistemas mediante protocolos ICMP, SNMP.

  - Control de acceso a los dispositivos.

  - Para el equipamiento de hardware se debe considerar también temperatura, uso de recursos (CPU-Memoria-Almacenamiento, etc.).

  - Chequeo de servicios de internet (Web, SMTP, SAMBA, NFS, DNS, entre otros).

  - Disponibilidad de aplicaciones: Apache, IIS, Bases de datos, Antivirus, entre otros.

- Los registros deben estar protegidos contra manipulación, pérdida o robo.

- Los registros solo deben ser accesibles a personal técnico y aquel autorizado por el comité de seguridad.

12.3.13 Comunicaciones

El SGSI aplicado a las comunicaciones busca la protección de la información en redes y cualquier otro medio de comunicación de la organización.

12.3.13.1 Gestión de redes

Objetivo: Garantizar el correcto funcionamiento de las redes de datos y voz y la seguridad de los datos transmitidos a través de ellas.

Responsable: Departamento de TI.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones asignadas.

En relación con la seguridad de las redes Telemarketing S.A.S deberá considerar:

- Documentar los procedimientos para la gestión de equipos informáticos en remoto, equipos de comunicaciones y las redes de voz y datos.
- Documentar los procedimientos para la revisión de registros\logs.
- Documentar los procedimientos de monitorización de las redes.

12.3.13.2 Gestión de transferencia de información

Objetivo: Garantizar que los medios y métodos para la transferencia y uso de información sea seguro.

Responsable: Toda la organización.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones asignadas

En la transferencia de información, se tendrán en cuenta los siguientes criterios con el fin de mantener los niveles de seguridad:

- Las políticas para el intercambio de información deberán estar documentadas y actualizada.
- El intercambio de información debe quedar registrado, incluyendo:

- Tipo de información.
- Medio de transmisión.
- Origen.
- Destino.
- Autorización.

- El uso de medios removibles (Memorias USB, Discos Duros Externos, Discos Ópticos, entre otros) estarán restringidos por defecto y se habilitarán solo para casos en los que sea requerido para la ejecución normal de las actividades y bajo la autorización del responsable de seguridad de la información o el comité de seguridad.

- Los usuarios son responsables de su uso y cuidado de los medios de transmisión de información, por tal razón deben mantenerlos en un lugar seguro y fuera del alcance de personal no autorizado.

- Los medios de transporte de información deben ser protegidos y embalados adecuadamente cuando sea necesario.

- Debe contarse con el acuse de recibido en el intercambio de información.

- Todos los soportes en medio electrónico deberán ser revisados para prevenir la presencia de código malicioso.

- Los soportes en medio electrónico deberán estar cifrados en la medida de lo posible. Esto es obligatorio cuando la información es de naturaleza confidencial.

- El uso de internet estará restringido y controlado según las necesidades de los usuarios para la normal gestión de sus actividades y siempre asociado a las actividades laborales, quedando prohibido el uso de este recurso (y los otros asignados por la empresa) para actividades personales.

12.3.13.3 Gestión de mensajería electrónica

Objetivo: Prevenir el uso no autorizado o inseguro de los medios de mensajería electrónica y garantizar la seguridad de la información en el uso de estos.

Responsable: Toda la organización.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones asignadas.

En relación con la gestión de mensajería electrónica se debe tener en cuenta los siguientes criterios:

- Los medios de correo electrónico son personales e intransferibles, se debe garantizar el control de acceso respectivo que permita, entre otras cosas, identificar siempre el remitente de la información.

- Las aplicaciones para el envío de la información deberán dejar un registro auditable de las actividades realizadas.

- Cuando se transmita información confidencial se deben usar mecanismos de encriptación y, en lo posible, de firma digital.

- En lo posible se debe asegurar que la plataforma de correo electrónico sea accesible solo desde las instalaciones de la organización.

- Se debe tener una política de contraseñas para el sistema de mensajería electrónica que tenga en cuenta como mínimo:

    - Longitud mínima de la contraseña.

    - Combinaciones requeridas.

    - Palabras y combinación de caracteres no admitidos.

    - Tiempo de renovación de contraseña.

- La información que se transmite por mensajería electrónica se hará única y exclusivamente por las cuentas de correo corporativas, quedando completamente prohibido el uso de cuentas personales para las labores.

- La cuenta de correo corporativo se usará única y exclusivamente para actividades laborales, quedando totalmente prohibido su uso para fines personales, para el envío de correos masivos (incluso dentro del índole laboral el envío de correos masivos será controlado), mensajes de carácter religioso, político, propagandístico o cualquier otro que no esté relacionado con las actividades de la empresa o que ponga en riesgo su reputación y buen nombre.

12.3.14 Proveedores

Se deben mantener los niveles de seguridad apropiados en la relación con terceros o proveedores.

12.3.14.1 Gestión de proveedores

Objetivo: Garantizar una relación segura con los proveedores, en la cual se garantice la seguridad de la información y de los activos y servicios que la soportan.

Responsable: Departamento de TI, Dirección de la organización, Departamento de Finanzas\Compras.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones asignadas En caso grave la anulación de los contratos.

En la gestión de proveedores se debe considerar lo siguiente:

- Se deben contemplar dentro de los procedimientos los servicios ofrecidos a TI por proveedores externos.
- Se debe contar con un procedimiento y planeación para la gestión de los proveedores en el cual se involucre:
    - Supervisión del rendimiento de los proveedores.
    - Revisión de los SLA de los proveedores.
    - Informes y reportes del SLA de los proveedores.
    - Revisión anual de los contratos con los proveedores.

12.3.15 Adquisición, desarrollo y mantenimiento de sistemas

Objetivo: Garantizar que se cumplen con políticas de seguridad de la información en los sistemas de información.

Responsable: Departamento de TI.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones asignadas.

El proceso de adquisición, desarrollo y mantenimiento de sistemas debe considerar:

- Debe existir un inventario o relación de los sistemas que se encuentran operativos en la organización.
- Debe existir la relación de las características de los sistemas actuales, así como el rendimiento actual y las proyecciones de crecimiento o modificaciones.
- Debe definirse los criterios que deben cumplir los sistemas que se van a implantar en la empresa (nuevos o actualizaciones), como:
    - Tipos de licencias.
    - Sistema de actualizaciones.
    - Intercambio de información, exportación o importación de esta.
    - Interfaces.

12.3.15.1 Gestión de nuevos sistemas de información y mejoras

Objetivo: Garantizar que se cumplen con políticas de seguridad de la información en los sistemas de información.

Responsable: Departamento de TI.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones asignadas.

La gestión de nuevos sistemas de información y mejoras debe considerar:

- Debe existir un inventario o relación de los sistemas que se encuentran operativos en la organización.
- Debe existir la relación de las características de los sistemas actuales, así como el rendimiento actual y las proyecciones de crecimiento o modificaciones.
- Los nuevos sistemas de información deben estar completamente documentados.
- Las mejoras o solicitudes de mejoras deben estar documentadas y justificadas.

12.3.15.2 Control de cambios

Objetivo: Definir correctamente los procedimientos necesarios ante las solicitudes de cambios en los sistemas de información.

Responsable: Departamento de TI.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones asignadas.

Los cambios en los sistemas de procesamiento y los servicios informáticos deberán ser controlados, teniendo en cuenta:

- Aspectos técnicos.
- Aspectos de seguridad.
- Procedimientos de implementación.

12.3.15.3 Control de instalación de software

Objetivo: Garantizar la correcta gestión en la instalación de software dentro de la organización.

Responsable: Departamento de TI.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones asignadas.

Con el fin de proteger los sistemas informáticos y la información de la organización, se debe documentar los controles en la instalación de software que incluyan entre otros:

- La instalación de software en los equipos de la organización solo podrá ser realizada por el personal de soporte técnico de IT o personal técnico especializado autorizado por el Responsable de Seguridad de la Información.
- La instalación de software nuevo deberá estar justificada y ser acorde con los requerimientos para la normal operación del centro.
- En caso de software propietario, la instalación debe estar respaldada por las licencias respectivas, considerando:
    - El tipo de licencia es acorde con el uso que se va a realizar.
    - Se debe contar con el medio que respalde la legalidad de la licencia (etiqueta, documento, etcétera).
    - Se debe acompañar de la factura u otro documento que respalde la obtención del software.
    - El software en prueba no será usado para la operación normal del centro.
- En caso de software open source o similar:
    - La empresa debe cumplir con las políticas de uso establecidas por el software o el desarrollador.
    - Las políticas de uso deben ser acordes con las políticas de la organización y con la legislación vigente.

- Las modificaciones de software tipo open o similares deben respetar los lineamientos de la comunidad open source y del desarrollador.

- El software instalado en los equipos personales de los empleados o en los equipos de proveedores y visitantes deben ser legales, el ingreso de equipos a la organización que no son propiedad de la empresa debe ir acompañado de un documento firmado por el propietario en el que certifique que el software que usa cumple con las condiciones de legalidad y derechos de autor, a su vez que exonera a la Telemarketing S.A.S de cualquier responsabilidad en caso de incumplimiento, siendo el propietario el único responsable ante cualquier implicación legal o sanción derivado del uso de software pirata.

Adicionalmente los nuevos aplicativos deberán pasar por las siguientes fases antes de su entrada en producción (también aplica para actualizaciones de estos):

- Fase de Preproducción: Todos los aplicativos nuevos, o las actualizaciones de ellos, deberán validarse en ambiente de preproducción donde se pueda verificar el correcto funcionamiento, su completa integración con los sistemas actuales y la no existencia de conflictos con otros aplicativos.

  También debe validarse que el hardware sobre el que se soportan los sistemas nuevos o actualizados sea suficiente para su correcto funcionamiento.

- Fase de Aceptación: Los aplicativos que han superado la fase de preproducción ser probados por usuarios seleccionados del área operativa\administrativa, quienes en base a unos criterios establecidos de aceptación probarán las funcionalidades del sistema y darán el visto bueno para la entrada en producción de los nuevos sistemas.

- Fase de regresión: Se deberá realizar pruebas en las cuales se valide el método a aplicar en caso de tener que realizar una regresión en la implementación de software nuevo o en la actualización de un aplicativo, verificar que dicha regresión no interrumpe la operación normal de la organización y en el caso que sea necesario, la forma en que se gestionaran los posibles inconvenientes que la regresión pueda provocar.

- Todas las fases deben estar documentadas y registradas.

12.3.16 Incidentes de seguridad

En este apartado se busca determinar los procesos para la identificación, escalado, comunicación, gestión y resolución de las incidencias de seguridad.

12.3.16.1 Gestión de incidentes de seguridad

Objetivo: Garantizar que los eventos e incidentes de seguridad son informados y tratados de forma adecuada a través de acciones correctivas y preventivas.

Responsable: Departamento de TI.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones asignadas.

En la gestión de los incidentes de seguridad se debe tener en cuenta lo siguiente:

- Se debe tener definido un proceso para el reporte de incidentes de seguridad que incluya lo siguiente:
    - El incidente debe ser reportado de tal forma que sea identificable, con todo el nivel de detalle posible y se pueda realizar seguimiento.
    - El responsable de la resolución de la incidencia se debe identificar.
    - Definir los mecanismos de comunicación de la incidencia, de tal forma que sean accesibles, disponibles y fáciles de usar.
    - El proceso debe incluir los pasos para el escalado de la incidencia.
    - Debe quedar trazabilidad de la incidencia.
    - El procedimiento debe estar disponible para todos los miembros de la organización.
    - Deben estar correctamente definidos los niveles de criticidad de los incidentes de seguridad de la información.

- Deben estar correctamente definidos los tiempos de respuesta (SLA's) de acuerdo con los niveles de criticidad.

- Se debe definir un protocolo o procedimiento relativo a la actuación frente a un incidente de seguridad considerando:

  - Detención de actividades en sistema afectado.
  - Desconexión y aislamiento del sistema afectado.
  - Análisis, valoración y calificación del incidente.
  - Comunicación de la incidencia a las partes interesadas (reporte de incidencia).

- Se debe contar con un protocolo o procedimiento relativo a la recolección y almacenamiento de evidencias en casos de incidentes de seguridad de tal forma que tengan validez en caso de iniciarse procesos disciplinarios o judiciales.

- Se debe realizar un análisis de los incidentes para generar acciones preventivas que permitan evitar la ocurrencia de dichos incidentes o similares.

12.3.16.2 Gestión de correcciones antes incidentes de seguridad

Objetivo: Garantizar una correcta gestión de las correcciones requeridas antes un incidente de seguridad con el fin de proteger los sistemas frente a amenazas detectadas.

Responsable: Departamento de TI, Comité de Seguridad.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones asignadas.

El Departamento de TI en conjunto con el Comité de Seguridad de Telemarketing S.A.S determinaran las condiciones y procedimientos mediante los cuales se aplicarán los cambios y actualizaciones requeridos ante la detección de riesgos de nivel elevado que afecten los sistemas de la organización de forma prioritaria. Se debe considerar:

- Los criterios por medio de los cuales se considera que el riesgo exige la aplicación de actualizaciones y correcciones de forma prioritaria.

- Los activos o sistemas informáticos sobre los que se aplicará la actualización o corrección de forma prioritaria.

- La gestión de autorizaciones para la aplicación de actualizaciones o correcciones prioritarias.

- El plan de trabajo para la aplicación de las fases de preproducción, aceptación y reversa para los casos de actualizaciones y/o correcciones prioritarias.

En general, todo riesgo que amenaza la operación de la organización o vulnera la disponibilidad, confidencialidad o integridad de los activos informáticos deberá ser resuelto de forma prioritaria.

12.3.17 Continuidad del negocio

El proceso de continuidad del negocio es el mecanismo por el cual la organización puede minimizar los efectos ante incidentes graves y/o pérdida de equipos que puedan impactar la operación, pudiendo mantener la operatividad en niveles aceptables mediante acciones preventivas y de recuperación. En este plan de continuidad, basado en la norma ISO 22301, se debe considerar los procesos de la organización (críticos), las políticas de seguridad de la información y lo relacionado con personal, materiales, transporte e instalaciones, de tal forma la restauración o reanudación de las actividades se de en un tiempo aceptable.

12.3.17.1 Gestión de la continuidad del negocio

Objetivo: Garantizar una correcta reacción ante eventos que puedan interrumpir la operación normal de la organización protegiendo los procesos críticos y asegurando una rápida reanudación de actividades.

Responsable: Departamento de TI, Dirección de la organización.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones asignadas.

En la gestión de la continuidad del negocio se deben considerar los siguientes criterios relacionados con la seguridad de la información:

- Desarrollar el plan de continuidad del negocio alineado con las políticas de seguridad de la información de la organización.

- Probar periódicamente el plan de continuidad del negocio y los procesos relacionados.

- El plan de continuidad del negocio debe estar integrado con los procesos de la organización.

- Implementar un grupo o comité encargado del plan de continuidad del negocio, su actualización y pruebas, con los siguientes roles definidos:

    - Equipo de gestión de crisis (CMT): Responsable de tomar las decisiones estratégicas.

    - Jefe de CMT: jefe responsable del equipo de gestión de crisis.

    - Responsable de infraestructura: Encargado de coordinar la seguridad de la información y garantizar la operatividad del centro de datos.

    - Equipo operacional: Personal de IT encargado de pruebas y las labores de recuperación.

    - Director de área: Responsable de área de negocio.

    - Personal general: todos los otros miembros de la organización.

12.3.17.2 Revisiones periódicas

Objetivo: Garantizar que la política de seguridad de la información se mantiene vigente, es revisada y se actualiza según los cambios en las condiciones del negocio o en las leyes relacionadas.

Responsable: Departamento de TI, Dirección de la Organización, Comité de Seguridad.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones asignadas.

Con el fin que el plan de contingencia se mantenga vigente y se pueda aplicar ante cualquier incidente que lo requiera, se debe mantener un plan de mantenimiento o revisiones periódicas.

- Implementar un plan de pruebas que incluya:
    - Verificación de flujos de entrada y salida de información.
    - Pruebas de aplicaciones y sistemas.
    - Participación de equipos de recuperación, responsables de área y personal directamente involucrado en el sistema que se prueba.
    - Ambiente de pruebas que abarque la mayor cantidad de escenarios posibles.
    - Corregir los puntos débiles del plan de acuerdo con las pruebas realizadas.
- Mantenimiento:
    - Reunión con los diferentes integrantes del equipo de gestión de crisis y los responsables de área para validar que conocen los procesos o reforzarlo según sea necesario.
    - Revisar el plan y actualizarlo\ajustarlo de acuerdo con las necesidades del negocio.
    - La revisión de plan de continuidad al menos una vez al año.
    - Se debe considerar revisiones del plan de forma extraordinaria cuando ocurran los siguientes eventos:
        - Cambios organizativos que involucren a los responsables de la continuidad del negocio.
        - Cambios en la infraestructura de la organización (física, voz, datos, etcétera).
        - Detección de problemas o resultados negativos en las revisiones periódicas del plan.
        - Cambios en los requerimientos de restauración para la continuidad del negocio.

- Implementación de nuevos aplicativos o software.
- Cambios a nivel de proveedores.

12.3.18 Cumplimiento

Telemarketing S.A.S debe tener un compromiso con el cumplimiento de las leyes, obligaciones legales o contractuales, o similares.

12.3.18.1 Cumplimiento de requisitos legales

Objetivo: Garantizar el cumplimiento de la legislación vigente respecto a seguridad de la información, seguridad informática y protección de datos personales.

Responsable: Departamento de TI, Dirección de la Organización, Comité de Seguridad.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones asignadas.

Dentro del cumplimiento de los requisitos legales la organización debe tener en cuenta lo siguiente (sin excluir otras normas vigentes para el tipo de organización que constituye Telemarketing S.A.S o su objetivo de negocio):

- Derechos de propiedad intelectual:
    - Para instalar software en la organización se debe cumplir con lo siguiente:
        - El software debe contar con una licencia en vigor.
        - En el caso de software libre la licencia debe ser adecuada para el entorno empresarial y debe ser probado.
        - En caso de software con licencia Shareware solo será instalado si el periodo de prueba no tiene fecha de caducidad, su funcionalidad es suficiente para los requerimientos y ha sido evaluado y aprobado por el departamento de IT.

- La instalación de software en los equipos de la organización solo puede ser realizada por el equipo de soporte técnico.

- El software instalado debe ser usado solo para fines laborales.

- Protección de datos personales:

  - Se deben contemplar en los procedimientos los requerimientos y lineamientos de la ley de protección de datos personales vigente en el país.

  - Las modificaciones en los sistemas de información deben ser acordes con los lineamientos de seguridad en relación con la protección de los datos personales.

  - Las medidas de seguridad serán acordes a los niveles de clasificación de la información:

    - Nivel básico: Ficheros con datos de carácter personal.

    - Nivel medio: Ficheros con datos relacionados con infracciones\investigaciones administrativas y penales, tributarias, servicios financieros, y similares.

    - Nivel alto: Ficheros relacionados con ideología religiosa, política, origen racial, salud o vida sexual o los relacionados con investigaciones policiales y judiciales.

12.3.19 Gestión de los registros y auditoría

12.3.19.1 Revisión por la Dirección

Objetivo: Garantizar que la política de seguridad de la información se mantiene vigente, es revisada y se actualiza según los cambios en las condiciones del negocio o en las leyes relacionadas.

Responsable: Departamento de TI, Dirección de la Organización, Comité de Seguridad.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones asignadas.

El proceso de revisión por la dirección será llevado a cabo de forma periódica con el fin que este actualizado y acorde con los cambios de la organización. El proceso de revisión debe contemplar lo siguiente:

- Los cambios en las políticas de seguridad se pueden presentar en las siguientes situaciones:
    - Solicitudes de las áreas o unidades directivas las cuales serán analizadas por el Departamento de TI.
    - Hallazgos realizados por parte del Departamento de TI en revisiones previas, incidentes, etcétera.
    - Solicitudes del Comité de Seguridad de la Información.
    - Cambios en la legislación y regulaciones.
    - Cambios en los procesos de negocio.

- El Departamento de TI será el encargado de revisar los cambios solicitados y aplicarlos en el documento. Cada revisión o cambio deberá incluir:
    - Numero de revisión\cambio.
    - Fecha de revisión\cambio.
    - Descripción del cambio.
- El documento con los cambios deberá ser revisado y aprobado por el comité de seguridad de la información.
- El documento será revisado con una periodicidad mínima de dos años.
- Se deberá contemplar y documentar en procesos los casos en que el documento deba ser revisado\aprobado por una entidad externa.
- Posterior a la aprobación se deberá comunicar a la organización las políticas de seguridad y los cambios presentados por parte del Comité de Seguridad de la Información.

Los procesos de revisión deberán estar acompañados por procesos de auditoría que cumplan con los siguientes criterios:

- Se debe tener definido un procedimiento de auditoría interna, preparado y mantenido por el Comité de Seguridad.

- Se debe contar con un cronograma anual de auditorías preparado por el Comité de Seguridad.

- El alcance de la auditoría debe contemplar, entre otros aspectos, lo siguiente:

    - Políticas y procedimientos.

    - Desarrollo y mantenimiento de programas.

    - Seguridad física: control de acceso, protección de activos.

    - Seguridad lógica: acceso a sistemas, acceso de usuarios, gestión y control de base de datos, redes y comunicaciones.

    - Internet y comercio electrónico.

    - Protección de propiedad intelectual, piratería, licenciamiento de software.

    - Protección de datos personales.

    - Contratos externos.

    - Procedimientos de copias de respaldo.

- Las pruebas de auditoría que involucren sistemas críticos deberán ser planificadas para evitar interrupciones de servicio.

- Los sistemas de información con datos personales serán auditados por una entidad externa que verifique el cumplimiento en materia de protección de datos personales.

- Los informes de la auditoria relacionada con datos personales será revisado por el Responsable de Seguridad de la Información y se aplicaran las acciones correctivas necesarias.

12.3.19.2 Auditoria

Objetivo: Medir el grado de cumplimiento del Sistema de Gestión de Seguridad de la Información para realizar las acciones correctivas y preventivas necesarias.

Responsable: Departamento de TI, Dirección de la Organización, Comité de Seguridad, Equipo Auditor

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones asignadas.

Telemarketing S.A.S deberá realizar procesos de auditoría considerando los siguientes criterios:

- Se deberán ejecutar dos procesos de auditoría completa al año (cómo mínimo), aunque con la posibilidad de realizar auditorías parciales que permitan validar el correcto funcionamiento del sistema en procesos específicos. Se **recomienda** que la ejecución del proceso de auditoría sea llevada a cabo al menos una vez al año por un ente externo (como complemento a los procesos internos).

  Considerar que ante un proceso de certificación de la norma ISO 27001 se deberán realizar las auditorias exigidas por el ente certificador en las fechas y con la periodicidad exigida por ellos.

- Los procesos de auditoría deberán ser llevados a cabo por personal calificado para esta labor, además de ser independientes de las áreas a auditar evitando el conflicto de intereses.

- Los procesos de auditoría que sean llevados a cabo en la organización deberán estar debidamente registrados y documentados, incluyendo la siguiente información:

  - Información de las personas u organización externa que realiza la auditoría.

  - Fecha de ejecución de la auditoría.

  - Motivo de ejecución de la auditoría (actividad programada, actividad relacionada con certificación, actividades de revisión parcial por cambios, actividades de revisión parcial por incidentes, entre otros).

  - Documentación de las No Conformidades, observaciones y/o hallazgos encontrados en el proceso de auditoría.

- Los hallazgos realizados en la ejecución de una auditoría deberán ser informados al Comité de Seguridad, y en caso necesario, al Comité Directivo de la organización.

- Los procesos de auditoría se apoyarán en las herramientas idóneas y probadas para llevar a cabo estas actividades, como son:
    - Formatos y registros desarrollados para estas actividades.
    - Software de detección de vulnerabilidades.
    - Software de análisis de redes.

12.3.20 Plan de recuperación de desastres

Objetivo: Contar con un plan que permita a la organización el restablecimiento de sus operaciones principales en caso de contingencia.

Responsable: Departamento de TI, Dirección de la Organización, Comité de Seguridad.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones asignadas.

Telemarketing S.A.S definirá un plan de recuperación de desastres (PRD) considerando lo siguiente:

- Considerar la infraestructura y procesos de la organización.
- Describir de forma detallado las acciones o pasos a ejecutar por la organización cuando se presenta una contingencia y se requiere restablecer las funciones principales de la empresa.
- El PRD debe estar alineado con el plan de continuidad de la empresa.
- El PRD debe estar acompañado por un análisis de impacto.
- El PRD debe ser probado periódicamente, y en los casos que se considere pertinente será modificado tras el análisis el Comité de Seguridad realice sobre los resultados de las pruebas y simulacros ejecutados.
- Se requiere que los Directivos de las áreas de la organización conozcan y sepan como ejecutar el PRD.

12.4 FORMACIÓN

Objetivo: Asegurar que los empleados, contratistas y usuarios externos estén capacitados y conscientes sobre las amenazas y preocupaciones relativas a la seguridad de la información, sus responsabilidades y obligaciones y estar preparados para apoyar la gestión de la política de seguridad. Igualmente se encuentren capacitados para el uso de las herramientas tecnológicas de la organización.

Responsable: Departamento de Gestión de Talento Humano y Departamento de TI en la organización de las capacitaciones; Todo el personal en la participación y cumplimiento de lo indicado en las capacitaciones.

Sanciones: Las estipuladas por el Departamento de Gestión de Talento Humano en relación con el incumplimiento de funciones asignadas. En el caso de empleados externos\internos y/o proveedores el incumplimiento puede acarrear la anulación del contrato.

Telemarketing S.A.S contará con los siguientes elementos para el personal contratado en la organización y para los proveedores:

- Procedimiento y plan de capacitación en Seguridad de la Información para el personal recién vinculado.
- Cronograma de reinducción en materia de seguridad de la información para el personal ya vinculado a la organización.
- Material informativo y de difusión sobre seguridad de la información.
- Registro de las acciones llevadas a cabo en materia de capacitación en seguridad de la información.

Los procesos de formación serán llevados a cabo por personal capacitado de TI, por el Departamento de Formación con el apoyo de TI, considerando lo siguiente:

- Las formaciones y el material usado deberán ser actualizado periódicamente, especialmente con base en los incidentes que se han detectado en la organización.

- Las formaciones deberán ser reforzadas periódicamente, como mínimo una vez al año.

- Las formaciones deberán culminar con aplicación de evaluación que incluya:

    - Evaluación para el equipo de formación por parte de los asistentes.

    - Evaluación para los miembros de la organización que reciben la formación.

    - Las evaluaciones del personal interno, externo y proveedores deben considerar un criterio mínimo de aprobación.

    - La no aprobación de las evaluaciones del personal interno, externo y proveedores debe desencadenar acciones correctivas y preventivas, tal como reinducción, o en casos críticos el cese de actividades del personal.

13 RESULTADOS

De acuerdo con los objetivos planteados se han realizado las actividades necesarias para alcanzar el diseño del SGSI para la organización Telemarketing S.A.S. En este proceso se han conseguido los siguientes resultados:

- Levantamiento de inventario: Se genera en conjunto con el Departamento de TI de la organización el cual se refleja en el capítulo 7 Inventario de activos, y con más detalle en el cuadro 8. Inventario de activos y valoración.

  El inventario desarrollado incluyo los activos que tienen relación con la información, es decir aquellos que procesan, almacenan y transportan, siendo clasificados de la siguiente forma:

  - Activos esenciales: Servicios de telefonía, LAN (Voz y Datos), marcador telefónico y base de datos operativa. Estos activos son fundamentales para la operación de la organización.

  - Personal: incluye el recurso humano operativo (agentes\ejecutivos), administrativo y el personal de estructura operativa.

  - Instalaciones: abarca el edificio general, los centros de datos o CPD, y las locaciones operativas y administrativas.

  - Servicios subcontratados: servicios de mantenimiento, página web, servicio de correo electrónico y de líneas telefónicas móviles.

  - Servicios internos: También se consideran, como ítem aparte, los servicios internos de configuración, servidor de archivos, bases de datos administrativas, entre otros.

  - Aplicaciones: Este ítem incluye el software ofimático, antivirus y las aplicaciones especializadas para gestión del talento humano, finanzas o actividades administrativas.

  - Equipos: hace relación tanto con equipos de usuario final, servidores. También, en un apartado independiente, se relacionan el equipamiento auxiliar que facilita la operación general de la organización (SAI, generador eléctrico, el cableado eléctrico, cableado de comunicaciones, impresoras y servicios de backups).

El equipamiento de comunicaciones también es parte del inventario (switches, firewall, canales de internet, MPSL y cableado estructurado voz/datos).

Durante el levantamiento de inventario se realiza valoración de los activos, tomando en cuenta la relevancia que tiene el activo en la operación de la organización, o, en otras palabras, el impacto que tendría para la empresa que un activo desaparezca o deje de funcionar. Esto ha permitido identificar:

- Los activos relacionados con la operación tienen valores altos, pues su afectación arriesgaría todas las actividades de la organización. Esta valoración cubre por ejemplo la red de datos, equipos servidores, equipos de comunicaciones, entre otros.

- Los activos de soporte a la operación, entre ellos los administrativos, tienen una calificación media.

- Otros servicios reciben calificaciones más bajas, según su relación con las operaciones principales de la organización.

- Análisis de riesgos y amenazas: Tomando como guía la metodología Magerit se ha realizado el análisis de amenazas y riesgos expuesto en el capítulo 8. Para completar el análisis se realizó lo siguiente:

  - Se realiza valoración de probabilidad de ocurrencia en una escala de 0,01 (Casi ninguna – Extremadamente difícil) a 100 (Diario – Fácil). Esto se expresa en el cuadro 9.

  - Tomando la tabla de activos se ha calculado el nivel de degradación y de impacto posible, lo cual se puede visualizar en el cuadro 10.

  - Por último, se calcula el nivel de riesgo tomando en cuenta el impacto y la frecuencia, dando como resultado el cuadro 11.

  Es importante señalar que para el cálculo de degradación e impacto se ha considerado que para algunos activos existen ya medidas de protección, por lo que su valoración puede ser alta pero su nivel de impacto, degradación o riesgo puede ser significativamente bajo.

- Identificación de problemas: Mediante el análisis de riesgos realizado se han identificado los problemas que existen en la organización relacionados con la seguridad de la información. Entre estos se puede destacar:

- Existen riesgos altos derivados por la falta de capacitación del personal de la organización en temas de seguridad de la información o incluso por el uso no adecuado de los recursos informáticos existentes.

- No existe un control preciso en el uso de los recursos, lo cual deriva en mal uso de los activos, falta de trazabilidad y autenticidad y posibles problemas de disponibilidad.

- Hay un riesgo importante relacionado con la gestión de copias de seguridad, asociado además a falta de conocimiento de los usuarios en cuanto al uso y generación de los backups.

El capítulo 9 abarca con más detalle los problemas detectados.

- Selección de políticas y controles: Como resultado de las actividades desarrolladas en el capítulo 8 y 9 se han elegido una serie de controles y políticas que serán consideradas en la fase de diseño del SGSI. Dicha selección se ha realizado buscando mitigar los riesgos detectados y se han plasmado en el cuadro 14 del capítulo 10.

  La selección de los controles y políticas se han apoyado en una clasificación en niveles de madurez representados en el cuadro 13 y que van en una escala de L0 (Inexistente) a L5 (Optimizado). Si bien existen ya controles implementados, ninguno alcanza el nivel optimizado y deben ser desarrollados de mejor forma; sobra decir que aquellos con niveles bajos como L0 o L1 es imprescindible que sean gestionados en la organización.

- Roles: En el capítulo 11 se han descrito los roles propuestos para el SGSI, considerando el organigrama actual de la organización, las posibilidades en cuanto a estructura de la empresa y las responsabilidades actuales de los miembros de la Telemarketing S.A.S.

Finalmente, con base en los ítems anteriores, se ha procedido a dar cumplimiento al objetivo general del proyecto consistente en el diseño del sistema de gestión de seguridad de la información para la empresa Telemarketing S.A.S considerando los siguientes ítems:

- Dentro del diseño se ha desarrollado la política general del sistema, el alcance y los objetivos del SGSI. Este punto da los lineamientos generales que debe cumplir el SGSI dentro de la organización, así como el papel que las directivas de Telemarketing S.A.S deben cumplir para la futura implementación del sistema y su sostenimiento en el tiempo.

- Se ha definido el alcance del SGSI al departamento de TI de Telemarketing S.A.S.

- Se han desarrollado las diferentes políticas que componen el SGSI considerando las salvaguardas, políticas y controles seleccionados en el capítulo 10 y de las cuales en un futuro se desprenderán los procesos, procedimientos, registros, formatos y otras medidas que harán parte del Sistema y permitirán la protección de la información y de los activos relacionados.

- El diseño concluye con los lineamientos relacionados con la formación del personal, punto importante para el éxito del SGSI y para su cumplimiento.

14 RECOMENDACIONES

Con base en las actividades realizadas en el proyecto, la información recolectada de las encuestas realizadas en la organización, los resultados del análisis de riesgos, la selección de las salvaguardas y políticas, se plantean una serie de recomendaciones para la organización.

En relación con el levantamiento de la información se recomienda:

- Mantener un inventario actualizado de los activos informáticos de Telemarketing S.A.S. Este inventario debe considerar:
    - Incluir los responsables o propietarios del activo.
    - Incluir fecha de compra\alta del activo. También se debe considerar como parte del activo la documentación que lo acompañe de tal forma que sea fácil su relación (ejemplo, la factura de compra de un servidor, su certificado de garantía, entre otros, deben ser fáciles de relacionar al activo, deben estar correctamente almacenados y debe ser sencilla su ubicación).
    - Incluir la ubicación del activo.
- Se recomienda además de tener un procedimiento para la baja del activo un proceso para su disposición final que también sea responsable con el medio ambiente y con la legislación vigente.

En relación con el análisis de riegos, la identificación de problemas y la selección de políticas y controles:

- Se recomienda realizar revisiones periódicas de los análisis de riesgos y amenazas previos con el fin de validar que se cuenta con las políticas y controles suficientes.
- Se recomienda, ante nuevas amenazas que surjan o que sean publicadas en revistas especializadas y relacionadas con SGSI, hacer una validación de los análisis previos para identificar si es necesario realizar una adaptación o nuevos cálculos y actuar en consecuencia de ello.

En relación con el diseño del SGSI se recomienda:

- Naturaleza de la organización: El sector en el cual se desenvuelve la organización (Centros de contacto), el uso de información personal, además de ser de cierta forma la representante comercial de las empresas para las cuales brindan servicios, implica entonces:

    - Considerar las regulaciones vigentes sobre protección de datos personal.
    - Considerar las regulaciones vigentes a nivel comercial, estatal, entre otras.
    - Seguir las regulaciones relacionadas con software legal.
    - Considerar las regulaciones respecto a contratación de personal interno y externo, así como contratación con proveedores.

  Es importante señalar que el mayor porcentaje de los empleados de la organización hace parte del área operativa, aproximadamente algo más del 50% de la plantilla corresponde a ejecutivos de atención de Contact center, el restante corresponde a supervisores, jefes de área, áreas de calidad y formación y personal administrativo, entre otros. Es importante reforzar las medidas que se tomen en relación con el SGSI con el área operativa debido a tres factores: a) Tienen contacto directo con usuarios a través de canales telefónicos (u otros como chat, email, etcétera), b) Tienen contacto directo con datos personales de estos usuarios y c) presentan una alta rotación (Aproximadamente el 47% del personal de la organización no tiene más de un año laborando en la empresa, este comportamiento es típico en este sector empresarial).

- Uso de la información: Las labores realizadas en la organización involucra el uso de información personal y corporativa. Es importante tener en cuenta que Telemarketing S.A.S ofrece sus servicios a otras empresas, dichos servicios consisten en atender los clientes de esas empresas para brindarles atención comercial, soporte técnico, etcétera. En este sentido un empleado de Telemarketing S.A.S tiene acceso a la información tanto de la empresa (para la cual se presta el servicio) como para el cliente de esta. Teniendo en cuenta lo anterior se recomienda:

- Restringir al máximo el uso de medios extraíbles de los ejecutivos de atención, incluso de supervisores, auditores de calidad, formadores, y cualquier otro cargo que no pueda justificar el uso de estos elementos.

- Disponer para los empleados todos los medios necesarios para la ejecución de sus labores, considerando especialmente que sean medios seguros para la información y evitar cualquier elemento que pueda ser usado para el robo\filtración de información.

- Implementar mecanismos de cifrado de la información, especialmente para datos sensibles.

- Implementar mecanismos de clasificación de la información, totalmente claros y que sean de conocimiento del personal, considerando al menos la información de carácter confidencial, interna y pública.

- Implementar medios de backup que permitan el respaldo seguro y el acceso controlado a la información. Desarrollar planes de respaldo de la información, así como controles y/o pruebas periódicas de los respaldos.

- Usar firmas digitales para los documentos que lo requieran, de tal forma que se pueda validar su procedencia e integridad.

- Cumplimiento de documentación: Respecto a la documentación se ha detectado que la organización no cumple con el 76% de la documentación indicada por la norma ISO 27001:2013, cumple parcialmente con el 21.4% y un 2.4% de la documentación no aplica por la naturaleza de la empresa. Considerando esto se recomienda considerar dentro de la documentación:

    - Política de seguridad.

    - Publicación de las políticas de seguridad.

    - Control de acceso.

    - Criptografía.

    - Operaciones.

    - Adquisición, gestión y mantenimiento de equipos.

    - Incidentes de seguridad.

    - Plan de Contingencia.

- Plan de Continuidad.

- Cumplimiento.

Adicionalmente es necesario que se cuente con revisiones periódicas, divulgación de la información y la actualización de la documentación de acuerdo con la evolución del SGSI, cambios en legislación, etcétera.

Igualmente, importante es la gestión de formatos y el registro de actividades, personal, incidentes o cualquier tipo de información señalada en los procedimientos y políticas de seguridad de la información.

- Teletrabajo: Algo más del 50% del personal manifiesta realizar teletrabajo, por lo cual es importante considerar las siguientes recomendaciones:

    - Intentar, en lo posible, replicar las condiciones de trabajo de los empleados en sus hogares (desde donde realizan sus labores), esto implica tanto los medios técnicos como las medidas de seguridad.

    - Para las conexiones a los sistemas de la empresa y clientes implementar comunicaciones vía VPN.

    - Implementar software de control en los equipos (computadores y teléfonos móviles) para el teletrabajo remoto.

    - Asignar actividades y labores acorde con las medidas de seguridad establecidas para la protección de la información.

    - Establecer clausulas especiales para la protección de la información en los contratos con personal que lleva a cabo teletrabajo.

- Relativa al personal: Debido a la alta rotación de personal y las operaciones que realizan en sus labores y/o el uso que hacen de datos de tipo personal o críticos de las organizaciones para las cuales brindan servicios:

    - Realizar (y reforzar periódicamente) las capacitaciones al personal de la organización en uso de tecnología general (uso correcto de ordenadores, periféricos, cuidados, entre otros), software de uso general (programas ofimáticos, antivirus, navegadores, entre otros), software de uso específico (software de marcador, aplicaciones de clientes).

    - Realizar (y reforzar periódicamente) capacitaciones al personal de la organización en seguridad de la información y políticas de seguridad de la

organización. Adicionalmente enseñar sobre las buenas prácticas en seguridad y uso de la información, y en lo posible mantener al tanto de las amenazas y formas de mitigación.

- Contratos: Incluir dentro de los contratos con el personal las cláusulas de confidencialidad necesarias para proteger los activos de información.

- Relativa al personal externo: Respecto al personal externo, es decir empleados de la organización contratados mediante outsourcing, pero también de los proveedores que están relacionados o brindan servicios a la organización, se debe considerar:

  - Capacitación: Incluir al personal externo, tanto como sea posible, en las capacitaciones que se realizan al personal interno, especialmente en lo que a seguridad de la información se refiere.

  - Contratación: Incluir en los contratos establecidos con el personal externo las cláusulas necesarias para salvaguardar y/o proteger los activos de la información. Esto implica el uso de cláusulas de confidencialidad (también aplicables al personal interno) para la protección de los activos de información, donde además se indique las consecuencias del incumplimiento de dichas cláusulas.

  - Control de acceso: También se debe definir las áreas accesibles y las no habilitadas para personal externo, especialmente para los proveedores quienes deberán tener una zona de carga y descarga específica (cuando se trata de proveedores de insumos) o zonas de circulación y trabajo (cuando se trata de proveedores de servicios). Así mismo se debe especificar las condiciones de acceso a los recintos para el personal externo como el uso de carné indicando claramente que se trata de proveedor, visitante, outsourcing, etcétera, y en el caso de proveedores, se debe contemplar claramente el personal interno que deberá acompañarlos durante la ejecución de sus labores.

- Relativa al uso de equipos (hardware) para la operación: En relación con los equipos con los cuales opera el personal, bien sea de tipo fijo como computadores de escritorio, o móviles tales como computadores portátiles, tabletas y teléfonos móviles, se realizan las siguientes recomendaciones:

  - Se debe mantener un inventario de todos los equipos que brindan operación a la empresa, tanto fijos como móviles. En el caso de equipos móviles, especialmente cuando son usados fuera de las instalaciones de la empresa, se debe mantener un registro de ellos donde se indique el responsable de/los equipo(s), las características de los mismos, números de

identificación y condiciones en que fueron entregados; también se debe incluir el anexo en el contrato de los empleados que reciben estos equipos las condiciones de uso y las consecuencias por el deterior por el mal uso, robo\perdida, entre otros.

- Todos los equipos de trabajo deben tener software licenciado y actualizado y deben estar controlados mediante el uso de usuario administrador. No se debe permitir la instalación de software diferente al autorizado por la organización, tampoco se debe permitir la instalación de hardware adicional en el equipo, y especialmente, las actividades técnicas (reparaciones, mantenimientos, diagnósticos) deben ser realizados exclusivamente por el área de IT o por proveedores autorizados por ellos.

- En lo posible, todos los equipos deben contar con las características físicas suficientes para la realización normal y fluida de las actividades laborales, es decir, deben ser equipos con el hardware suficiente y actualizado.

- El ingreso a todos los equipos, sean estos fijos o móviles, deberán implementar mecanismos y/o políticas de control de acceso mediante usuario y contraseña con el fin de gestionar el acceso a los servicios brindados por estos dispositivos y por las redes a los cuales están conectados.

- Para el software usado en los dispositivos y que tengan relación con la operación de la organización (correo electrónico, software de marcador telefónico, aplicaciones de clientes, entre otros) se recomienda el uso de autenticación en dos pasos.

- Se debe mantener un cronograma anual de mantenimiento de todos los equipos usados en la operación de la organización. Dicho cronograma debe contemplar una frecuencia suficiente de mantenimiento para garantizar el correcto funcionamiento de los equipos y debe cumplirse a cabalidad por el personal de IT o por los proveedores seleccionados para ello y debe incluir revisión tanto a nivel físico (hardware) como lógico (software).

- Para las personas que realizan teletrabajo se recomienda a la organización disponer de equipos propios para ellos, con todas las condiciones de los dispositivos usados internamente y el software de control y gestión necesarios para garantizar su uso eficiente en trabajo remoto.

- Todos los equipos deben contar con software para el control de aplicaciones maliciosas o dañinas (antivirus, antispam, antimalware, entre otros) incluidos los dispositivos móviles como tabletas y teléfonos celulares. Estos aplicativos deben estar licenciados y actualizados constantemente.

- Los equipos móviles, especialmente aquellos con los que se trabaje fuera de la empresa deben contar con encriptación para proteger la información que se guarde en ellos.
- Se recomienda a la organización mantener un stock de equipos de respaldo con las características suficientes y operativos, de tal manera que puedan reemplazar unidades defectuosas en el menor tiempo posible y con el menor efecto en la operación diaria.

- Se recomienda además evitar al máximo el uso de ordenadores o móviles personales para la realización de labores de la empresa. En caso de ser necesario el uso de estos equipos se debe garantizar que cumplan con todas las condiciones legales (especialmente en licenciamiento). Estos equipos deben quedar registrados.

- Hardware Crítico: Se considera como hardware crítico los equipos que brindan servicios fundamentales para la operación de la empresa como los servidores de bases de datos, de archivos, de aplicativos, switches, routers, firewalls, entre otros. Si bien estos equipos están protegidos por la empresa se considera oportuno recomendar:

  - Definir un cronograma anual en el cual se definan las actividades de revisión y mantenimiento de estos equipos. Velar por el cumplimiento de dicho cronograma y llevar un registro de las actividades.

  - Mantener un plan de renovación y actualización del hardware crítico con holgura suficiente para el crecimiento de las operaciones.

  - Mantener vigente el licenciamiento del software de los equipos críticos, así como los aplicativos para el control de software malicioso.

  - Definir con antelación ventanas de mantenimiento que no afecten la operación.

- Software: Muchas de las operaciones de la organización se respaldan sobre software especializado (marcadores telefónicos, bases de datos), software de uso general (software ofimático, sistemas operativos, entre otros) y algunas aplicaciones propias desarrolladas por el equipo de TI. Se hacen las siguientes recomendaciones:

  - Todo el software debe estar debidamente licenciado, las licencias deben mantener su vigencia y ser adecuadas para el tipo de uso de los aplicativos en la organización. En lo posible, sumado a la licencia contar con un plan de soporte del fabricante del software.

- El uso de software libre este sujeto a las condiciones del licenciamiento que lo acompaña, es decir que no se debe usar software cuyo licenciamiento libre no aplica para el uso empresarial o comercial.
- Los aplicativos con licencia de prueba (testing, periodo de prueba) solo serán válidos con fines de testeo y no deben ser usados para las operaciones normales de la empresa.

- Para el software se deberá tener un cronograma de mantenimiento y actualizaciones con una periodicidad suficiente para cubrir las necesidades de la organización. Siempre que el fabricante lo recomiende se deben instalar las últimas actualizaciones o parches para mejorar el rendimiento del aplicativo o corregir fallos, especialmente cuando están relacionados con la seguridad.

- La actualización de software deberá pasar por una etapa previa de prueba, donde las actualizaciones serán testeadas en equipos o ambientes de prueba antes que las actualizaciones y cambios sean aplicados de forma masiva a todos los dispositivos de la organización.

- Para el software desarrollado In-House se deberán considerar todas las buenas prácticas de desarrollo establecidos por organizaciones o grupos especializados en el tema.

- Los desarrollos internos deberán considerar la preservación de la disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad de la información.

- El código fuente de los desarrollos internos deberá estar respaldado y protegido del acceso de personal no autorizado.

- Redes de datos y telefonía: las redes de datos de la empresa, así como las de telefonía, son esenciales para la comunicación de los equipos de usuario final con los servicios y servidores. Para su buen funcionamiento y protección se recomienda:

  - Llevar anualmente un cronograma de mantenimiento, ejecutar las actividades allí establecidas, llevar un registro del resultado de los mantenimientos y reportar los problemas que sean detectados.

  - Controlar el acceso a la red de datos y telefonía, así como bloquear los puertos no usados en el caso de las redes físicas.

  - Para el caso de redes inalámbricas mantener un control de acceso con un sistema de seguridad robusto. Se debe separar las redes dentro de la organización mediante sistemas lógicos o virtuales (VLAN) para su uso

interno. El uso de personal externo (visitas, proveedores y actividades que no son parte de la operación) deben usar redes separadas o independientes.

- Relativo al uso de internet: Aunque en la encuesta realizada se considera el uso de internet como esencial en las labores se debe señalar que esta percepción puede no ser exacta, puesto que a) el software de marcación es un sistema instalado en los servidores propios de la empresa, b) Los servicios de telefonía son entregados por los proveedores a través de canales dedicadas empresariales, y c) el acceso a las herramientas o software de los clientes se realiza por medio de servicios dedicados de tipo MPSL. El internet es usado como complemento para el área operativa en algunos casos, mientras que el área administrativa usa algunos servicios específicos a través de la *World Wide Web*. Respecto a este servicio se entregan las siguientes recomendaciones:

    - Implementación de servidor proxy y firewall para el control y gestión del acceso a Internet. Es importante que estos servicios estén operativos y actualizados, así como mantener un buen control de las listas de sitios permitidas y las denegadas (las cuales deben ser actualizadas periódicamente).

    - En lo posible implementar control de acceso para el uso de Internet.

    - Controlar el uso de los canales de internet para que su uso sea acorde con los requerimientos de la organización.

- Respecto a las credenciales de acceso: El uso de credenciales de acceso debería ser obligatorio para todo el personal tanto para el uso de hardware (Computadores, tabletas y teléfonos celulares) como de software (programas de cliente, propios, etcétera). Se recomienda lo siguiente:

    - En los equipos que se usan internamente en la organización se recomienda implementar servicios de directorio activo para la gestión de las credenciales de acceso, y se debe capacitar a los usuarios en el correcto uso de ellas.

    - En los equipos externos usar métodos de autenticación suficientes para proteger el acceso a los mismos.

    - En la medida de lo posible implementar autenticación de dos pasos para el acceso a software.

- Tanto a nivel de hardware como de software, se recomienda implementar el cambio obligatorio de contraseñas de forma periódica, de ser posible con una frecuencia no mayor a 3 meses.

- Los equipos deberían contar con bloqueo automático cuando no están siendo usados después de un periodo de tiempo, en lo posible, no mayor a 3 minutos.

- Incidentes de seguridad: Los incidentes de seguridad hacen parte del día a día, algunos son ignorados por el personal en general mientras que otros se materializan para ellos, y en este último caso es importante el manejo que se den, por ello se realizan las siguientes recomendaciones:

    - Capacitar al personal en SGSI, amenazas/riesgos, incidentes de seguridad. En esta capacitación se debe tener en cuenta la forma en que se deben reportar estos incidentes y a quien se debe reportar (conocer el equipo encargado de la seguridad de la información de la empresa).

    - Se recomienda instruir al personal sobre pasos básicos o iniciales antes un incidente de seguridad: cambio inmediato de contraseñas, desconexión de equipos de la red de datos y voz, análisis con software antivirus y antimalware, reporte del incidente al personal encargado de seguridad de la información o a IT, entre otras medidas que se consideren necesarias.

    - Es importante que el área de IT realice una revisión de las publicaciones de los medios especializados sobre seguridad informática\seguridad de la información para estar al tanto de novedades. Adicionalmente mantener contacto con algunas entidades relacionadas con SGSI, facilitar el intercambio de conocimiento, participar de eventos (Congresos, capacitaciones, entre otros).

    - Como parte de las medidas de contingencia el área de TI, así como el área administrativa debe mantener un directorio actualizado con las diferentes organizaciones de emergencia de la ciudad (Policía, Bomberos, Clínicas) como también de servicios básicos y relacionados con la operación (acueducto, energía, telefonía, entre otros) con el fin de poder actuar rápidamente ante una contingencia. Mantener contacto con estas organizaciones para estar al tanto de las novedades que se puedan presentar.

- Uso de medios extraíbles: El uso de medios extraíbles, considerando la naturaleza de la organización y el manejo de datos personales y confidenciales debería estar limitado al máximo dentro de la organización. Las siguientes recomendaciones están relacionadas con el uso de medios extraíbles:

- Bloquear en los equipos de operación el acceso a puertos de lectura/escritura de medios extraíbles. Estos puertos solo deben estar habilitados para personal que demuestre suficientemente la necesidad de acceso a estos medios de almacenamiento y deben estar registrados debidamente para que puedan ser identificados fácilmente y relacionados con los computadores en los cuales dispongan de estos permisos.

- Registrar todos los medios extraíbles que se utilizan dentro de la empresa identificando su propietario, área a la que pertenece, el uso que se la da frecuentemente, fecha de compra y, cuando aplique, fecha de baja y disposición final.

- Los medios extraíbles usados en la organización deberán contar con encriptación.

- Los medios extraíbles de personal externo o visitante a la organización solo podrán ser leídos\grabados por personal de IT, que previamente revisará con software de detección de código malicioso el medio.

- Instalaciones físicas: Si bien las instalaciones físicas no están expuestas de forma significativa a amenazas (de acuerdo con el análisis realizado) se recomienda lo siguiente:

    - Separación de espacios según las labores que se realizan y los activos que contienen, asegurando la protección de la información y de los medios que los contienen y los sistemas (y los soportes) que los procesan.

    - Los espacios deben estar debidamente señalizados con el fin que sean identificables por todo el personal, además de indicar las zonas de acceso prohibido o restringido.

    - Los espacios críticos no deben tener libre acceso, deben estar asegurados con puertas y sistemas de apertura suficientes para controlar el acceso a estas zonas. En general se recomienda como medida de seguridad abarcar todas las zonas posibles en el circuito cerrado de televisión (CCTV) y llevar registro de los accesos a las zonas restringidas.

    - Se deben instalar equipos de detección ante situaciones de amenaza como detectores de humo, detectores de agua o control de humedad, detectores de movimiento para controlar el acceso a zonas restringidas, entre otros. Igualmente contar con sistemas de protección como extintores, sistemas de rociadores de agua, tableros de control eléctrico, etcétera. Todos estos sistemas deben abarcar todas las áreas de forma suficiente y estar 100%

operativos, y además contar con cronogramas de mantenimiento y registro de actividades.

- Logs y ficheros de configuración: Como parte de las medidas de seguridad se debe considerar el cuidado de los logs y ficheros de configuración, por tal razón se realizan las siguientes recomendaciones:

    - Se debe mantener un respaldo de los ficheros de configuración de los equipos, especialmente aquellos que cumplen una función importante en la operación como servidores, firewall, switches, routers, modems, entre otros. Antes de realizar cambios en la configuración de los equipos se debe respaldar la configuración vigente, igualmente posterior a las acciones de mantenimiento\cambios realizar copia de seguridad y almacenarla.

    - Se debe mantener un respaldo de los logs que se generan en los sistemas y/o equipos críticos.

    - Se debe mantener una revisión periódica de los logs de los sistemas y equipos críticos con el fin de identificar problemas o vulnerabilidades. Se debe llevar un registro de las revisiones.

    - En los aplicativos (software) desarrollados In-House se debe incluir un módulo de registro de logs para las acciones importantes o que tengan relación con la manipulación de la información.

Como recomendación general es importante que la organización, en especial las directivas, estén comprometidas al 100% con el SGSI. El sistema de gestión de seguridad de la información no es estático, debe ser analizado y mejorado constantemente para que ese adapte a los cambios que se presentan en el mundo tecnológico y la empresa debe destinar los recursos necesarios para que esto se cumpla.

Es además importante que el personal de la organización este familiarizado con el SGSI mediante los procesos de formación\capacitación, pero además que se les genere una cultura de cumplimiento y respeto hacía el mismo. El crecimiento de la organización debe ir acompañado de la evolución del sistema de gestión de seguridad de la información, esta es la mejor forma de garantizar su éxito y que perdure en el tiempo.

15 CONCLUSIONES

El proyecto llevado a cabo con la empresa Telemarketing S.A.S ha permitido identificar intentos previos de implementar algo cercano a un Sistema de Gestión de Seguridad de la Información con el fin de dar cumplimiento a los requerimientos de los clientes para los cuales ofrecen servicios, sin embargo se requiere dar un paso más allá para tener un SGSI completo dado que existen aún requerimientos, procesos y controles que falta por implementar o aplicar dentro de la empresa y de esta forma garantizar que se puede cumplir con la integridad, confidencialidad y disponibilidad de la información (sumado a la autenticidad y trazabilidad). En este sentido, el proyecto ha realizado las diferentes etapas que permiten llegar al diseño del SGSI y en este trayecto se han logrado las siguientes conclusiones:

- La organización objeto de este proyecto (y cualquier otra) cuenta con activos informáticos de diferente naturaleza y protagonismo en las actividades que se realizan, he incluso se pueden encontrar diferentes esfuerzos en protegerlos y velar por su correcto funcionamiento dentro de las operaciones. No obstante, se evidencia que Telemarketing S.A.S requiere mejorar en este ítem para que la información sea fiable y completa, así como contar con los datos necesarios para estar en capacidad de realizar una valoración más precisa.

- El análisis de riegos desarrollado permitió trazar un camino para llegar al objetivo de diseñar el SGSI para la organización. En este camino se identificaron las vulnerabilidades, las amenazas y se calcularon los riesgos. No obstante, este es un proceso que debe continuar trabajando de tal forma que se actualice y ajuste de acuerdo con los cambios internos y externos de la empresa; el análisis era prácticamente inexistente en la organización, ahora existe una base sobre la cual se deberá continuar trabajando y ajustando a la realidad de Telemarketing S.A.S.

- El levantamiento del inventario de activos, junto con el análisis de riesgos y la posterior identificación de problemas ha permitido identificar falencias importantes de cara al diseño de un Sistema de Gestión de la Seguridad de la Información que llegue a ser funcional: a) La falta de documentación de procesos, controles y políticas, b) La falta de aplicación de controles establecidos en la norma ISO\IEC 27001:2013, c) las deficiencias en la capacitación de los empleados y la difusión de las políticas de seguridad de la información, d) la ausencia los métodos de protección de la información y de los activos que los procesan y almacenan, como los sistemas de respaldo (Backups), los controles de acceso o incluso las actividades de mantenimiento y adquisición de hardware y software.

- Aunque en la organización existen ya documentos (procedimientos, formatos, políticas) previos, estos eran insuficientes para considerarse como SGSI, no obstante con el trabajo realizado se han seleccionado las políticas y controles necesario para la empresa que además permitirán definir y desarrollar los documentos que a día de hoy no existen, o solo cubren parcialmente con los requerimientos; dicha selección se ha realizado en base a los análisis de riesgos y amenazas, de tal forma que respondan a los problemas detectados pero también que sean aplicables y viables para la organización. Es importante señalar que para incluir un SGSI dentro de una empresa se requiere hacer un esfuerzo significativo partiendo desde un análisis a conciencia de la organización que permita llegar a establecer los controles y políticas pertinentes, y por ello además, se requiere de orden u organización para que los datos para dicho análisis estén disponibles y puedan ser medidos, y en lo posible apoyarse en documentos (formatos, registros, entre otros) que sirvan como soporte y respaldo, así como fuente de información; ya esta tarea se ha avanzado de forma significativa en el presente proyecto y dependerá de Telemarketing S.A.S completarla en miras de lograr la implementación del sistema.

- Parte fundamental del éxito en la implementación del SGSI dependerá de un esfuerzo importante de la organización en la capacitación o formación de sus empleados en políticas del SGSI y otros temas relacionados con la seguridad de la información puesto que sus altos niveles de rotación hacen que el personal operativo cambie de forma significativa en plazos que incluso no son superiores a un año. De hecho, no basta con la capacitación inicial que se imparte al ingreso de personal nuevo, sino que es necesario realizar actividades de refuerzo en las cuales a) se recuerde a los miembros de la organización de las políticas de seguridad de la información y b) se actualice sobre los cambios en el SGSI, el uso de tecnología e información e incluso sobre riesgos y amenazas que han surgido con el pasar del tiempo y la forma de gestionarlos. Sin embargo, no se puede olvidar que existe otra parte importante para el éxito del SGSI y este tiene que ver con los roles que cumple cada integrante en el sistema, partiendo de las directivas de la organización, de quienes debe partir el ejemplo en la aplicación y cumplimiento de las políticas de seguridad de la, pero además deben dar el apoyo suficiente en logística y recursos para llevar a cabo la tarea de implementación del sistema de forma satisfactoria. Se suma el rol y el compromiso que deben cumplir los miembros del Comité Directivo que permita reflejar hacía el resto de la organización la importancia de la seguridad de la información, de la protección de los datos y de los activos informáticos, del cumplimiento de los procedimientos y del acatamiento de las normas, incluidas las leyes vigentes en relación con la protección de datos personales, licenciamiento legal, entre otros.

BIBLIOGRAFÍA

ACUNETIX. Directory Traversal Attacks. {En línea}. Diponible en: (https://www.acunetix.com/websitesecurity/directory-traversal/).

AFP. Wikileaks publica este lunes 1.7 millones de documentos diplomáticos. {En línea}. {07 de abril de 2013}. Disponible en: (https://www.elespectador.com/noticias/wikileaks/wikileaks-publica-lunes-17-milllones-de-documentos-dipl-articulo-414599).

ALMANZA JUNCO, Andrés Ricardo. Tendencias 2015 Encuesta nacional de seguridad informática: 15 años después . {En línea}. {Junio de 2015}. Disponible en: (https://acis.org.co/portal/sites/all/themes/argo/revista/Sistemas135.pdf).

ALMANZA JUNCO, Andres Ricardo. Encuesta nacional de seguridad informática 2017. {En línea}. {2017}. Disponible en: (http://acis.org.co/revista143/content/encuesta-nacional-de-seguridad-inform%C3%A1tica-2017).

ALMUNIA, Pablo. IEDGE: Estándares para la gestión de TI. {En línea}. Disponible en: (https://www.iedge.eu/pablo-almunia-estandares-para-la-gestion-de-ti-primera-parte#comment-1736).

AVAST ACADEMY TEAM. Ingeniería Social. {En línea}. {19 de mayo de 2020}. Disponible en: (https://www.avast.com/es-es/c-social-engineering).

BRICEÑO, Eduardo. Guía de la semana: Qué es la ingeneiría social y como estar prevenidos. {En línea}. {25 de abril de 2012}. Disponible en: (https://hipertextual.com/archivo/2012/04/que-es-la-ingenieria-social-y-como-estar-prevenidos/).

BSI Group. Nuestra historia, los inicios, el desarrollo y el hoy. {En línea}. Disponible en: (https://www.bsigroup.com/es-MX/acerca-de-BSI/Nuestra-historia/).

CALIDAD & GESTION. Ciclo PDCA: Estrategía para la mejora continua. {En línea}. Disponible en: (http://www.calidad-gestion.com.ar/boletin/58_ciclo_pdca_estrategia_para_mejora_continua.html).

CAZARAN BUITRAGO, Olger Yonatan. Diseño de un sistema de gestión de seguridad de la información en el área de recursos informáticos en la Contraloría Departamental del Meta, según la norma ISO 27001. Villavicencio, 2017, 106p.Trabajo de grado para optar por el título de: Especialista en Seguridad Informática. Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnología e Ingeniería. Disponible en: (https://repository.unad.edu.co/bitstream/10596/17423/1/1121839952.pdf).

CESPI UNLP. Incidentes informáticos. {En línea}. Disponible en: (https://cespi.unlp.edu.ar/incidentes).

CHAUI. Cobit 5: Fundamentos de facilitadores / habilitadores / catalizadores. {En línea}. {15 de mayo de 2015}. Disponible en: (https://chaui201511700911004.wordpress.com/2015/05/15/cobit-5-fundamentacion-de-facilitadores-habilitadores-catalizadores/).

CIFUENTES, Andres. Retos de ciberseguridad para las compañias en el 2018. {En línea} {22 de diciembre de 2017}. Disponible en: (http://gerente.com/co/rciberseguridad-companias-2018/).

CONGRESO DE LA REPUBLICA. Ley 1245 por la cual se establecen normas para promover y regular el teletrabajo y se dictan otras disposiciones. {En línea}. {06 de octubre de 2008}. Disponible en: (http://www.informatica-juridica.com/anexos/Ley_1221_de_16_de_julio_de_2008.asp).

CONGRESO DE LA REPUBLICA. Ley 1273 de 2009 por medio de la cual se modifica el código penal, se cra un nuevo bien jurídico tutelado: denominado de la protección de la información y los datos. {En línea}. {05 de enero de 2009}.Disponible en: (http://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf).

CONGRESO DE LA REPÚBLICA. Ley 1273 de 2009 por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado: denominado de la protección de la información y de los datos . {En línea}. {05 de enero de 2009}. Disponible en: (http://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf).

CONGRESO DE LA REPUBLICA. Ley 23 del 28 de Enero de 1982 sobre derecho de autor. {En línea}. {28 de enero de 1982}. Disponible en: (http://www.informatica-juridica.com/anexos/Ley_23_28_enero_1982_derecho_autor.asp).

CONGRESO DE LA REPUBLICA. Proyecto de Ley 241 por el cual se regula la responsabilidad por las infracciones de derecho de autor y los derechos conexos en internet. {En línea}. {04 de abril de 2011} Disponible en:. (http://servoaspr.imprenta.gov.co/gacetap/gaceta.mostrar_documento?p_tipo=05&p_numero=241&p_consec=28543).

CONBRESO DE LA REPUBLICA. Proyecto de Ley No. 227.{En línea}. {21 de abril de 1998}. Disponible en: (http://www.informatica-juridica.com/anexos/Proyecto_Ley_N%C2%BA_227_Abril_21_1998_Comercio_Electronico.asp).

CORLETTI ESTRADA, Alejandro. ISO 27001: Los Controles (Parte 1). {En línea}. (Noviembre de 2006). Disponible en: (http://www.iso27000.es/download/ISO-27001_Los-controles_Parte_I.pdf).

DE CONCEPTOS. Concepto de estándar. {En línea}. Disponible en: (https://deconceptos.com/ciencias-sociales/estandar).

DIP, Patricia. Dato e Información. {En línea}. {13 de abril de 2008}. Disponible en: (http://latecnologiavirtual.blogspot.com/2008/04/dato-e-informacin.html).

DUQUE OCHOA, B R. Metodologías de gestión de riesgos (OCTAVE, MAGERIT, DAFP). {En línea}. Disponible en: (https://auditoriauc20102mivi.wikispaces.com/file/view/Metodologìas+deGestiòn+de+Riesgos.pdf).

FIGOLI PACHECO, A. El acceso no autorizado a sistemas informáticos. {En línea}. Disponible en: (http://www.buscalegis.ufsc.br/revistas/files/anexos/2778-2772-1-PB.htm).

FUNDACIÓN UNIPYMES. Empresas Colombianas más involucradas con la transformación digital. *Unipymes.* {En línea}. {21 de noviembre de 2019}. Disponible en: (https://www.unipymes.com/empresas-colombianas-mas-involucradas-con-la-transformacion-digital/).

GUZMÁN GARCÍA, Alexánder y TABORDA BEDOYA, Carlos Alberto. Diseño de un sistema de gestión de la seguridad informática -SGSI-, para empresas del área textil en las ciudades de Itagüi, Medellín y Bogotá D.C a través de la auditoría. Bogotá D.C, 2015, 311p. Trabao de grado para optar el título de Especialización en Seguridad Informática.

Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnología e Ingeniería. Disponible en: (http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3448/1/1030548291.pdf).

HADOPI. Haute Autoritépour la diffusion des ceuvres et la protection des droits sur internet. {En línea}. Disponible en: (https://www.hadopi.fr/en/haute-autorite/about-hadopi).

ICDE. Estándares. {En línea}. Disponible en: (http://www.icde.org.co/web/guest/wiki/-wiki/Wiki%20de%20la%20ICDE/Est%C3%A1ndares).

INFOBAE. Suicidios, chantajes y un mapa de infieles, entre las consecuencias del ataque a Ashley Madison. {En línea}. {24 de agosto de 2015}. Disponible en: (https://www.infobae.com/2015/08/24/1750447-suicidios-chantajes-y-un-mapa-infieles-las-consecuencias-del-ataque-ashley-madison/).

INVIMA. Política de Seguridad de la Información. {En línea}. {16 de enero de 2017}. Disponible en: (https://www.invima.gov.co/images/stories/formatotramite/GDIDIEPL010version2.pdf).

ISACA. ¿Qué es COBIT y para qué sirve?. {En línea}. {27 de septiembre de 2016}. Disponible en: (https://nextech.pe/que-es-cobit-y-para-que-sirve/).

ISO 27000.ES. ISO 27000. {En línea}. {2005} Disponible en: (http://www.iso27000.es/iso27000.html).

ISO 27000.ES. Origen. {En línea}. Disponible en: (http://www.iso27000.es/iso27000.html#seccion1).

ISO Tools Excellence.. ISO 27001. Origen e historia.. {En línea}. {10 de diciembre de 2013}. Disponible en: (https://www.pmg-ssi.com/2013/12/iso27001-origen/).

ISO TOOLS Excellence. Los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad. {En línea}. {01 de febrero de 2018}. Disponible en: (https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/).

ISO27000.ES. Glosario. {En línea}. Disponible en: (http://www.iso27000.es/glosario.html).

ISOTools Excellence. ¿Cuáles son las medidas para reforzar la ciberseguridad?. {En línea}. {15 de noviembre de 2018}. Disponible en: (https://www.pmg-ssi.com/2018/11/cuales-son-las-medidas-para-reforzar-la-ciberseguridad/).

ISOTools Excellence. ISO 27001: Los activos de información. {En línea}. {30 de marzo de 2015}. Disponible en: (https://www.pmg-ssi.com/2015/03/iso-27001-los-activos-de-informacion/).

ITIL BOOKS. How is ITIL organized. {En línea}. Disponible en: (http://www.itil.org.uk/how.htm).

KASPERSKY. Qué es el Cibercrimen: Definición. {En línea}. Disponible en: (https://www.kaspersky.es/resource-center/threats/cybercrime).

LISA INSTITUTE. Guía práctica contra la ingeniería social. {En línea}. {08 de mayo de 2020}. Disponible en: (https://www.lisainstitute.com/blogs/blog/guia-practica-ingenieria-social).

LOPEZ, Miguel. !A cubierto¡: Telegram esta sufriendo un ataque DDoS a escala global. {En línea}. {10 de julio de 2015}. Disponible en: (https://www.genbeta.com/mensajeria-instantanea/a-cubierto-telegram-esta-sufriendo-un-ataque-ddos-a-escala-global).

LORENZO PEREZ, Alfonso. Riesgo, amenaza y vulnerabilidad. {En línea}. {26 de junio de 2018}. Disponible en: (https://eq2b.com/riesgo-amenaza-y-vulnerabilidad-iso-27001/).

MARQUIS, Hank. 10 Steps to Do It Yourself CRAMM.. {En línea}. {17 de diciembre de 2008}. Disponible en: (http://www.itsmsolutions.com/newsletters/DITYvol4iss50.pdf).

MASADELANTE. ¿Qué es un virus informático? {En línea}. Disponible en: (https://www.masadelante.com/faqs/virus).

MELON, Luis. Los 5 retos clave para la ciberseguridad en 2018. {En línea}. {12 de diciembre de 2017}. Disponible en: (https://ciberseguridad.blog/los-5-retos-clave-para-la-ciberseguridad-en-2018/).

MONTERO ABUJAS, David. Ingeniería social. {En línea}. {2017}. Disponible en: (https://es.slideshare.net/monteseugenio/owand11-granada-ingeniera-social).

OBS Business School. Las 3 metodologías para la gestión de proyectos que más se utilizan. {En línea}. Disponible en: (https://www.obs-edu.com/int/blog-project-management/administracion-de-proyectos/las-3-metodologias-para-la-gestion-de-proyectos-que-mas-se-utilizan).

OSIATIS. ¿Qué es ITIL? {En línea}. Disponible en: (http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/fundamentos_de_la_gestion_TI/que_es_ITIL/que_es_ITIL.php).

OWASP. Inyección SQL. {En línea}. Disponible en: (https://www.owasp.org/index.php/Inyecci%C3%B3n_SQL).

OWASP. Inyección SQL. *OWASP.* {En línea}. Disponible en: (https://www.owasp.org/index.php/Inyecci%C3%B3n_SQL).

PANDA MEDIA CENTER. ¿Qué es un troyano?. {En línea}. {10 de diciembre de 2013}. Disponible en: (https://www.pandasecurity.com/spain/mediacenter/consejos/que-es-un-troyano/).

PANDA SECURITY. Virús informático. {En línea}. Disponible en: (https://www.pandasecurity.com/es/security-info/virus/).

PDCAHOME. Las normas ISO más usadas. {En línea}. {27 de marzo de 2013}. Disponible en: (https://www.pdcahome.com/4168/las-normas-iso-mas-usadas/).

PEREZ SAN-JOSE, P, y otros. Estudio sobre riesgos de seguridad derivados del software no autorizado. {En línea}. {11 de junio de 2012}. Disponible en: (http://bibliotecaescolardigital.es/comunidad/BibliotecaEscolarDigital/recurso/estudio-sobre-riesgos-de-seguridad-derivados-del/61000a84-88e3-449e-83e8-e1a0e34d16ca).

PMG SGSI. ISO 27001: Origen e historia. {En línea}. {10 de diciembre de 2013}. Disponible en: (https://www.pmg-ssi.com/2013/12/iso27001-origen/).

POWERDATA. Transformación digital: Qué es y su importancia y relación con los datos. {En línea}. Disponible en: (https://www.powerdata.es/transformacion-digital).

RED IRIS. Seguridad física de los sistemas. {En línea}. {15 de julio de 2002}. Disponible en: (https://www.rediris.es/cert/doc/unixsec/node7.html).

REVISTA DINERO. Las empresas colombianan escatiman en gastos y se rajan en ciberseguridad. {En línea}. {19 de enero de 2017}. Disponible en: (https://www.dinero.com/empresas/articulo/encuesta-anual-de-seguridad-de-la-informacion-de-la-firma-ey/241201).

RIVERO, Marcelo. ¿Qué es el phishing?. {En línea}. Disponible en: (https://www.infospyware.com/articulos/que-es-el-phishing/).

SANDOVAL CASTELLANOS, Edgar Jair. Ingeniería social: corrompiendo la mente humana. {En línea}. Disponible en: (https://revista.seguridad.unam.mx/numero-10/ingenier%c3%ad-social-corrompiendo-la-mente-humana).

SECURITY, PANDA. Virús informático. {En línea}. Disponible en: (https://www.pandasecurity.com/es/security-info/virus/).

SEGURIDAD INFORMATICA. Herramienta de evaluación de riesgo: CRAMM. {En línea}. Disponible en: (https://seguridadinformaticaufps.wikispaces.com/Herramienta+de+Evaluacion+de+Riesgo-CRAMM).

SEGURIDAD PC. Concepto de troyanos informáticos. {En línea}. Disponible en: (http://www.seguridadpc.net/troyanos.htm).

SYMANTEC. Ataques DoS. {En línea}. Disponible en: (https://www.symantec.com/es/mx/security-center).

TANQUE DE ANÁLISIS Y CREATIVIDAD DE LAS TIC (TICTAC) - CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES CCIT. Informe Tendencias del CiberCrimen Primer Trimestre 2020. {En línea}. {Abril de 2020). Disponible en: (https://www.ccit.org.co/wp-content/uploads/informe-tendencias-abril-2020-final.pdf).

TANQUE DE ANÁLISIS Y CREATIVIDAD DE LAS TIC (TICTAC) - CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES CCIT. Tendencias Cibercrimen Colombia 2019-2020. {En línea}. {29 de octubre de 2019}. Disponible en: (https://www.ccit.org.co/wp-content/uploads/informe-tendencias-final.pdf).

ANEXO A. DIAGNÓSTICO INICIAL DOCUMENTACIÓN

Cuadro 15. Diagnóstico inicial de documentación

Clausula	Nombre	Calificación	Cumple
4.3	Alcance del sistema de gestión de seguridad de la información	Obligatorio	No
5.2\6.2	Política de seguridad de la información	Obligatorio	Parcial
5.2\6.2	Objetivos de la seguridad de la información	Obligatorio	No
6.1.2	Metodología de evaluación y tratamiento de riegos	Obligatorio	No
6.1.3d	Declaración de aplicabilidad	Obligatorio	No
6.1.3e\ 6.2	Plan de tratamiento de riesgos	Obligatorio	No
8.2	Informe sobre evaluación de riesgos	Obligatorio	No
A.7.1.2\ A.13.2.4	Definición de roles y responsabilidades de seguridad	Obligatorio	Parcial
A.8.1.1	Inventario de activos	Obligatorio	Parcial
A.8.1.3	Uso aceptable de los activos	Obligatorio	Parcial
A.9.1.1	Política de control de acceso	Obligatorio	Parcial
A.12.1.1	Procedimientos de operación para gestión de TI	Obligatorio	No
A.14.2.5	Principios de ingeniería de sistemas seguros	Obligatorio	No
A.15.1.1	Política de seguridad para proveedores	Obligatorio	No
A.16.1.5	Procedimiento para gestión de incidentes	Obligatorio	No
A.17.1.2	Procedimientos de continuidad de negocio	Obligatorio	No
A.18.1.1	Requerimientos legales, regulatorios y contractuales	Obligatorio	Parcial
7.2	Registro de formación, habilidades, experiencia y calificaciones	Obligatorio	Parcial
9.1	Seguimiento y resultados de medición	Obligatorio	No
9.2	Programa de auditoría interna	Obligatorio	No
9.2	Resultados de auditorías internas	Obligatorio	No
9.3	Resultados de revisión por la dirección	Obligatorio	No
10.1	Resultados de acciones correctivas	Obligatorio	No
A.12.4.1\A. 12.4.2	Registro de las actividades de usuario, excepciones y eventos de seguridad	Obligatorio	No
7.5	Procedimiento para control de documentos	No obligatorio	No
7.5	Controles para la gestión de registros	No obligatorio	No
9.2	Procedimiento para auditoría interna	No obligatorio	No
10.1	Procedimiento para acciones correctivas	No obligatorio	No
A.6.2.1	Política BYOD	No obligatorio	No aplica
A.6.2.1	Política de dispositivo sobre dispositivos móviles y teletrabajo	No obligatorio	Parcial
A.8.2.1\ A.8.2.2\ A.8.2.3	Política de clasificación de la información	No obligatorio	No

A.9.2.1\ A.9.2.2\ A.9.2.4\ A.9.3.1	Política de claves	No obligatorio	No
A.8.3.2\ A.11.2.7	Política de eliminación y destrucción	No obligatorio	No
A.11.1.5	Procedimientos para trabajo en áreas seguras	No obligatorio	No
A.11.2.9	Política de pantalla y escritorios limpios	No obligatorio	No
A.12.1.2\ A.14.2.4	Política de gestión de cambios	No obligatorio	No
A.12.3.1	Política de copias de seguridad	No obligatorio	Parcial
A.13.2.1\ A.13.2.2\ A.13.2.3	Política de transferencia de información	No obligatorio	No
A.17.1.1	Análisis de impacto en el negocio (BIA)	No obligatorio	No
A.17.1.3	Plan de pruebas y verificación	No obligatorio	No
A.17.1.3	Plan de mantenimiento y revisión	No obligatorio	No
A.17.1.2	Estrategia de continuidad de negocio	No obligatorio	No

Fuente: Propia

ANEXO B. DIAGNÓSTICO INICIAL PROCESOS Y DOMINIOS

Cuadro 16. Diagnóstico inicial políticas de seguridad de la información

Políticas de seguridad de la información		
Código	**Control**	**Cumple**
A.5.1.1	Cuenta la organización con políticas para la seguridad de la información	Si
A.5.1.2	Realiza la organización la revisión de las políticas de seguridad de la información	No
A.6.1.1	Se encuentran definidos los roles y responsabilidades para la seguridad de la información	Si
A.6.1.2	Existe segregación de funciones y áreas de responsabilidad para evitar conflictos	Si
A.6.1.3	Existe un directorio de contacto con autoridades relacionados con TI y SI. Existe un contacto con dichas autoridades	No
A.6.1.4	Existe un directorio de contacto con grupos de interese relacionados con TI y SI. Existe un contacto con dichos grupos	No
A.6.1.5	Se incluye la seguridad de la información en la gestión de proyectos	No
A.6.2	Se desarrolla operación mediante dispositivos móviles o teletrabajo	No

Fuente: Propia

Cuadro 17. Diagnóstico inicial de recursos humanos

Recursos Humanos		
Código	**Control**	**Cumple**
A.7.1.1	Se verifican los antecedentes de los posibles empleados de la organización de acuerdo con las legislaciones vigentes y los requisitos del negocio	Si
A.7.1.2	El contrato con los empleados y contratistas estipula las responsabilidades respecto a la seguridad de la información (acuerdos de confidencialidad, acceso a la información, etcétera)	Si
A.7.2.1	La gerencia exige a todos los miembros de la organización (empleados y contratistas) la aplicación\cumplimiento de directrices de seguridad de la información	No
A.7.2.2	La organización capacita a los empleados y contratistas en relación con seguridad de la información, actualización de políticas, etcétera	No
A.7.2.3	La organización cuenta un proceso disciplinario formal y comunicado que se lleva a cabo con los empleados que cometan infracción contra la seguridad de la información	Si
A.7.2.4	Existen clausulas posteriores a la finalización del contrato con el empleado que preserven la seguridad de la información y se hacen cumplir	No

Fuente: Propia

Cuadro 18. Diagnóstico inicial de gestión de activos

Gestión de Activos		
Código	**Control**	**Cumple**
A.8.1.1	Se cuenta con inventario de activos completo y actualizado	Parcial
A.8.1.2	Los activos cuentan con un propietario asignado	No
A.8.1.3	Existen reglas y procedimientos sobre el uso aceptado de la información y los	Si
A.8.1.4	Existe un procedimiento de devolución de activos y se cumple	Si
A.8.2.1	Se dispone de una clasificación clara de la información	Si
A.8.2.3	Existe un procedimiento para el etiquetado de la información y se aplica	No
A.8.2.4	Existen procedimientos para el manejo de la información	No
A.8.3.1	Existe un procedimiento para el uso de medios removibles	Si
A.8.3.2	Existe un procedimiento para la disposición final de medios removibles	No
A.8.3.3	Existe un procedimiento para el transporte de medios removibles protegiéndolos de acceso no autorizado, mal uso o corrupción de la información	No

Fuente: Propia

Cuadro 19. Diagnóstico inicial de control de acceso

Control de acceso		
Código	**Control**	**Cumple**
A.9.1.1	Existe una política de control de acceso a la información y a las instalaciones de procesamiento de la información (CPD)	No
A.9.1.2	Existen reglas\procedimientos que definan el acceso de los usuarios a la información y a los servicios de red	No
A.9.2.1	Existe un procedimiento para el alta y baja de usuarios	No
A.9.2.2	Existe un procedimiento para la asignación\revocación de permisos de acceso	No
A.9.2.3	Existe un procedimiento para la asignación\revocación de permisos de acceso privilegiados	No
A.9.2.4	Existe un proceso por medio del cual se entregue la información de autenticación secreta (claves)	No
A.9.2.5	Existe un proceso por medio del cual se revisen los accesos de los usuarios de forma periódica	No
A.9.2.6	Existe un procedimiento para la revocación definitiva de los accesos a la información y las instalaciones de procesamiento de la información	No
A.9.3.1	Existe un procedimiento sobre las prácticas en el uso de información de autenticación secreta	No
A.9.4.1	Se tiene definido las restricciones de acceso a la información y las funciones del sistema de acuerdo con las políticas de control de acceso	Si
A.9.4.2	Existen procedimientos de ingreso seguro a la información y las funciones del sistema de acuerdo con las políticas de control de acceso	No

Control de acceso		
A.9.4.3	Existe un sistema de gestión de contraseñas	No
A.9.4.4	Se tiene control y restricciones sobre los programas que funcionan con acceso privilegiado	Si
A.9.4.5	El código fuente de los programas se encuentra protegido y está restringido	Si

Fuente: Propia

Cuadro 20. Diagnóstico inicial de criptografía

Criptografía		
Código	**Control**	**Cumple**
A.10.1.1	Existe una política sobre el uso de controles criptográficos que involucre las laptops	Si
A.10.1.1	Existe una política sobre el uso de controles criptográficos que involucre los móviles	No
A.10.1.1	Existe una política sobre el uso de controles criptográficos que involucre dispositivos de almacenamiento externo	No
A.10.1.1	Existe una política sobre el uso de controles criptográficos que involucre la transmisión de información por medios electrónicos	No
A.10.1.2	Existe una política para la gestión de claves criptográficas que incluya el uso, protección y tiempo de vida	No

Fuente: Propia

Cuadro 21. Diagnóstico inicial de seguridad física

Seguridad Física		
Código	**Control**	**Cumple**
A.11.1.1	Existe un perímetro de seguridad definido para el edificio de tal forma que se proteja la información sensible o crítica y la infraestructura de procesamiento de datos	Si
A.11.1.1	Existe un perímetro de seguridad definido para el Centro de Procesamiento de Datos (CPD) que proteja la información sensible o crítica y la infraestructura de procesamiento de datos	Si
A.11.1.2	Existen controles para el acceso físico a las instalaciones de la empresa y las zonas críticas	Si
A.11.1.3	Existen controles de seguridad para las oficinas y otras áreas e instalaciones	Si
A.11.1.4	Existen controles y políticas relacionadas con la protección física de las instalaciones contra desastres naturales (inundación, fuego, tormenta, entre otras), ataques maliciosos (robos, asonadas) o accidentes	Si

Seguridad Física		
A.11.1.5	Existen procedimientos y controles para el trabajo en áreas seguras (CPD, Almacenamiento de archivos, entre otros)	No
A.11.1.6	Existe control y procedimientos para las áreas de despacho y carga, las zonas por las que personas no autorizadas pueden ingresar a las instalaciones o las zonas de procesamiento de datos	No

Fuente: Propia

Cuadro 22. Diagnóstico inicial de equipos

Equipos		
Código	**Control**	**Cumple**
A.11.2.1	La ubicación de los equipos informáticos es adecuada y se encuentran protegidos de amenazas, peligros y acceso no autorizado (Edificio)	Si
A.11.2.1	La ubicación de los equipos informáticos es adecuada y se encuentran protegidos de amenazas, peligros y acceso no autorizado (CPD)	Si
A.11.2.2	Los equipos informáticos cuentan con servicio de alimentación ininterrumpida y regulada (Edificio)	Si
A.11.2.2	Los equipos informáticos cuentan con servicio de alimentación ininterrumpida y regulada (CPD)	Si
A.11.2.3	El cableado eléctrico y de datos de la organización se encuentra debidamente protegido de daños e intervenciones	Si
A.11.2.4	Existe procedimiento\control\cronograma de mantenimiento de equipos	Si
A.11.2.5	Existe un procedimiento\control para el movimiento\traslado de equipos	Si
A.11.2.6	Existe un control y procedimiento para los equipos de la empresa que se encuentran fuera de las instalaciones	NO
A.11.2.7	Existe un procedimiento para los equipos de la empresa que serán reutilizados (incluye el borrado de información, gestión de licencias, etc.)	SI
A.11.2.8	Existen procedimientos\políticas para los equipos desatendidos y se hace cumplir	SI
A.11.2.9	Existe un procedimiento de escritorio y pantalla limpia	SI

Fuente: Propia

Cuadro 23. Diagnóstico inicial de operaciones

Operaciones		
Código	**Control**	**Cumple**
A.12.1.1	Los procedimientos a nivel operativo se encuentran documentados	No
A.12.1.1	Los procedimientos se encuentran disponibles para los usuarios involucrados	No
A.12.1.1	Existe un directorio de documentación	No

Operaciones		
A.12.1.2	Existe un control para la gestión de cambios en la organización, procesos de negocio, instalaciones y sistemas de procesamiento de información	No
A.12.1.3	Existe un control sobre el uso de los recursos, junto con una proyección de los requisitos de capacidad futura y los ajustes necesarios para garantizar la operación	No
A.12.1.4	Existe una separación de los ambientes de desarrollo, pruebas y producción	Si
A.12.2.1	Existen controles para la detección, protección, prevención y recuperación ante códigos maliciosos, así como actividades de capacitación para los usuarios	No
A.12.3.1	Existe un procedimiento de copias de respaldo de la información, del software, imágenes del sistema	No
A.12.3.1	Existe un procedimiento periódico de prueba de las copias de respaldo	No
A.12.4.1	Existe un procedimiento de registro de eventos sobre las actividades de los usuarios, fallos y eventos de la seguridad de la información.	No
A.12.4.2	Los registros y las instalaciones donde se contienen están protegidos contra alteración y acceso no autorizado	No
A.12.4.3	Existe un procedimiento de registro de eventos sobre las actividades del administrador y el operador	No
A.12.4.3	Los registros del administrador y el operador se encuentran protegidos y se revisan con regularidad	No
A.12.4.4	Los relojes de todos los sistemas de procesamiento (computadores, servidores, equipos de comunicaciones, etcétera) se encuentran sincronizados con una única fuente	Si
A.12.5.1	Existen procedimientos y controles sobre la instalación de software en sistemas operativos	Si
A.12.6.1	Se cuenta con información oportuna de las vulnerabilidades técnicas asociadas a los sistemas usados en la organización	No
A.12.6.1	En base a la información sobre vulnerabilidades técnicas se evalúa la exposición de la organización frente a ellas y se toman medidas	No
A.12.6.2	Se cuenta con restricciones y reglas para la instalación de software por parte de los usuarios	Si
A.12.7.1	Los procesos de auditoría que involucran los sistemas operativos son debidamente programados y desarrollados de tal forma que se afecte al mínimo la operación y los procesos del negocio	Si

Fuente: Propia

Cuadro 24. Diagnóstico inicial de comunicaciones

Comunicaciones		
Código	**Control**	**Cumple**
A.13.1.1	Existe control y correcta gestión de las redes por las cuales circula la información (protección, entre otros)	Si
A.13.1.2	Para todos los servicios de red (internos y externos) se identifican los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión, se incluyen en los acuerdos de servicio	Si
A.13.1.3	Los grupos de servicios de información, usuarios y sistemas de información se encuentran separados en las redes (VLAN)	Si
A.13.2.1	Existen políticas, procedimientos y controles de transferencia de información mediante el uso de instalaciones de comunicaciones (VPN)	Si
A.13.2.2	Existen acuerdos sobre la transferencia de información entre la organización y las entidades externas (clientes, proveedores, entre otros)	Si
A.13.2.3	Se protege adecuadamente la información enviada por mensajería electrónica	Si
A.13.2.4	Se cuenta con acuerdos de confidencialidad de la información los cuales son revisados y adaptados según las necesidades de la organización	Si

Fuente: Propia

Cuadro 25. Diagnóstico inicial adquisición, desarrollo y mantenimiento de sistemas.

Adquisición, desarrollo y mantenimiento de sistemas		
Código	**Control**	**Cumple**
A.14.1.1	Se incluyen los requisitos de seguridad de la información para los nuevos sistemas de información y para mejoras de los sistemas actuales	No
A.14.1.2	La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se encuentra protegida de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas	Si
A.14.1.3	La información involucrada en las transacciones de los servicios de las aplicaciones se encuentra protegidas para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada y la duplicación o reproducción de mensajes no autorizada	Si
A.14.2.1	Existen políticas y reglas para el desarrollo seguro de software y de sistemas, y son aplicadas	No
A.14.2.2	Existe un procedimiento formal para el control de cambios de los sistemas dentro del ciclo de vida de desarrollo	No
A.14.2.3	Existe un procedimiento de pruebas (test) en los cambios en las plataformas de operación para asegurar que no exista impacto adverso en las operaciones o seguridad de la organización (Aplicaciones Críticas del Negocio)	No
A.14.2.4	Existe un control estricto a los cambios o modificaciones sobre los paquetes de software, limitándolos a lo necesario	Si

Adquisición, desarrollo y mantenimiento de sistemas		
A.14.2.5	Existe un documento que define los principios de construcción de sistemas seguros, los cuales mantienen y se aplican a cualquier actividad de implementación de sistemas de información	No
A.14.2.6	Se cuenta con ambientes protegidos de desarrollo seguro para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas	Si
A.14.2.7	Existen procesos de desarrollo externo	No Aplica
A.14.2.7	Se tienen procesos de supervisión y seguimiento a los desarrollos de sistemas contratados externamente	No Aplica
A.14.2.8	Se cuentan con procedimientos de pruebas de funcionalidad de la seguridad para los sistemas	No
A.14.2.9	Se cuenta con procedimientos de pruebas para determinar la aceptación para los sistemas de información nuevos, actualizaciones y nuevas versiones	Si
A.14.3.1	Existen datos de prueba seleccionados, protegidos y controlados	Si

Fuente: Propia

Cuadro 26. Diagnóstico inicial de incidentes de seguridad

Incidentes de seguridad		
Código	**Control**	**Cumple**
A.16.1.1	Existe una asignación de responsabilidades y procedimientos de gestión de los incidentes de seguridad de la información	Si
A.16.1.2	Los eventos de seguridad son reportados a través de los canales de gestión apropiados	Si
A.16.1.3	Los empleados y contratistas reportan las vulnerabilidades y\o debilidades de la seguridad de la información	Si
A.16.1.4	Se evalúan y clasifican los eventos de seguridad	No
A.16.1.5	Se da respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados	No
A.16.1.6	Se usa y mejora la seguridad de la información a partir del conocimiento adquirido y la resolución de los incidentes de seguridad	No
A.16.1.7	Existen procedimientos documentados para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia	No

Fuente: Propia

Cuadro 27. Diagnóstico inicial de Proveedores

Incidentes de seguridad		
Código	**Control**	**Cumple**
A.15.1.1	Existen políticas de seguridad de la información para las relaciones con proveedores, acordados con estos y documentados	No

Incidentes de seguridad		
A.15.1.2	Los acuerdos con proveedores incluyen todos los requisitos de seguridad de la información pertinentes	Si
A.15.1.3	Los acuerdos con proveedores incluyen los requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro	No
A.15.2.1	Existe un proceso de auditoría, seguimiento y/o revisión de los servicios prestados por proveedores	Si
A.15.2.2	Existe un proceso de control y gestión de cambios en el suministro de servicios por parte de los proveedores	Si

Fuente: Propia

Cuadro 28. Diagnóstico inicial de continuidad

Continuidad		
Código	**Control**	**Cumple**
A.17.1.1	Se cuenta con una planificación que permita la continuidad de la gestión de la seguridad de la información en situaciones adversas	No
A.17.1.2	Se cuenta con los procesos (documentados), procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa	No
A.17.1.3	Se realizan revisiones periódicas de los controles de continuidad de la seguridad de la información	No
A.17.2.1	Las instalaciones de procesamiento de información cuentan con redundancia	Si

Fuente: Propia

Cuadro 29. Diagnóstico inicial de cumplimiento

Cumplimiento		
Código	**Control**	**Cumple**
A.18.1.1	Se han identificado, documentados y actualizados todos los requisitos estatutarios, reglamentarios y contractuales relacionados con la seguridad de la información y la organización	No
A.18.1.2	Se cumple con todos los requisitos de propiedad intelectual y el uso de productos de software patentados	No
A.18.1.3	Los registros se protegen contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada de acuerdo con las reglamentaciones y legislación	No
A.18.1.4	Se cumple con los lineamientos de privacidad y protección de la información de datos personales	Parcial
A.18.1.5	Se usan controles criptográficos según los acuerdos, legislación y reglamentación vigente	No
A.18.2.1	Existe independencia dentro de la organización para la revisión de la gestión de la seguridad de la información y su implementación	No

A.18.2.2	La dirección de la organización revisa con regularidad el cumplimiento del SGSI y los requisitos de seguridad	No
A.18.2.3	Se realizan revisiones periódicas del cumplimiento de las políticas y las normas de seguridad	No

Fuente: Propia

ANEXO C. INVENTARIO DE ACTIVOS

Cuadro 30. Inventario de activos

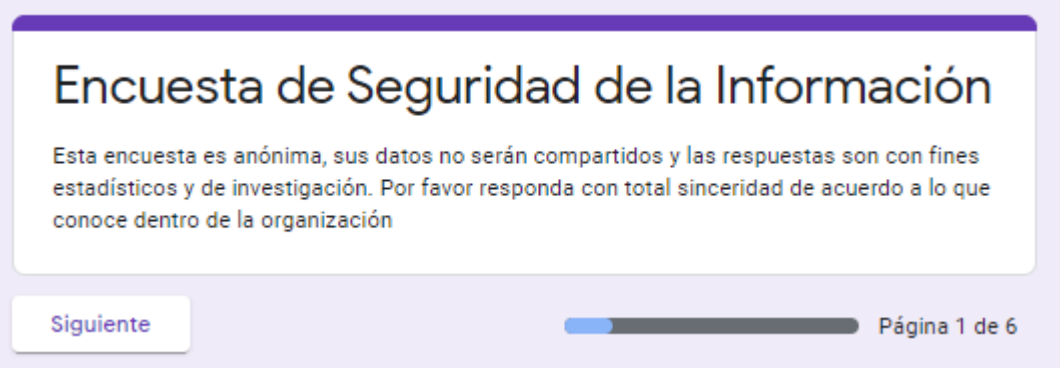
Grupo	Tipo	Identificador	Nombre
Esencial	S	S_TELEFONIA	SERVICIO DE TELEFONÍA
Esencial	S	S_LANOPERAT	RED LAN OPERATIVA VOZ Y DATOS
Esencial	S	S_GESTORTEL	SERVICIO DE GESTIÓN DE MARCACIÓN TELEFÓNICA
Esencial	IS	D_BDDATOSOPER	BASE DE DATOS OPERATIVA VOCALCOM\OCM
Personal	A	P_PERSOPER	PERSONAL OPERATIVO
Personal	A	P_PERADMIN	PERSONAL ADMINISTRATIVO RRHH\FINAN\IT\GERENCIA
Personal	A	P_ESTRUCOPER	PERSONAL ESTRUCTURA DE OPERACIÓN\CAL\FORM\REPORT
Instalaciones	A	L_EDIFGRAL	EDIFICIO GENERAL
Instalaciones	A	L_CPD	CENTRO DE DATOS
Instalaciones	A	L_SITEOPERADMIN	LOCACIONES OPERATIVAS Y ADMINISTRATIVAS
Serv. Subc	SS	SS_SERVGRALES	SERVICIOS GENERALES MANTENIMIENTO
Serv. Subc	SS	SS_WEB	SERVICIO DE PÁGINA WEB
Serv. Subc	SS	SS_EMAIL	SERVICIO DE CORREO ELECTRÓNICO
Ser. Subc	SS	SS_MOBILE	SERVICIO DE LINEAS MÓVILES
Equipamiento (SW)	A	SW_OFIMAT	SOFTWARE OFIMÁTICO
Equipamiento (SW)	A	SW_ANTIV	SOFTWARE ANTIVIRUS
Equipamiento (SW)	A	SW_ADMIN	SOFTWARE ADMINISTRATIVO CONTABILIDAD-RRHH-GESTIÓN
Equipamiento (HW)	A	HW_ORDENADOR	EQUIPOS DE ESCRITORIO-LAPTOPS
Equipamiento (HW)	A	HW_SERV	SERVIDORES

Grupo	Tipo	Identificador	Nombre
Equipamiento (HW)	A	HW_MOBIL	EQUIPOS DE TELEFONÍA MÓVIL
Equipamiento (AUX)	A	AUX_UPS	SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA
Equipamiento (AUX)	A	AUX_GEN	GENERADOR ELÉCTRICO DE RESPALDO
Equipamiento (AUX)	A	AUX_CABELEC	CABLEADO ELÉCTRICO CENTRO
Equipamiento (AUX)	A	AUX_FIB	CABLEADO FIBRA ÓPTICA
Equipamiento (AUX)	A	AUX_PRINT	IMPRESORAS OPERATIVAS Y ADMINISTRATIVAS
Equipamiento (AUX)	A	AUX_BACKUPS	SERVICIO DE BACKUPS
Equipamiento (COM)	A	COM_SWITCHES	SWITCHES CORE Y DISTRIBUCIÓN
Equipamiento (COM)	A	COM_FIREWALL	FIREWALL
Equipamiento (COM)	A	COM_INTER	CANAL DE INTERNET PRINCIPAL Y BACKUP
Equipamiento (COM)	A	COM_MPLSMAT	CANAL DE MPLS CASA MATRIZ PRINCIPAL Y BACKUP
Equipamiento (COM)	A	COM_LAN	CABLEADO ESTRUCTURADO VOZ Y DATOS
Servicios Internos (TECH)	A	IS_CONF	FICHEROS DE CONFIGURACIÓN
Servicios Internos (TECH)	A	IS_MANUAL	FICHEROS DE MANUALES Y PROCEDIMIENTOS
Servicios Internos	IS	IS_FILESERVER	SERVICIO DE SERVIDOR DE ARCHIVOS
Servicios Internos	IS	IS_SERVBBDD	SERVICIO DE BASES DE DATOS ADMINISTRATIVO Y APOYO OPERATIVO

Fuente: Propia

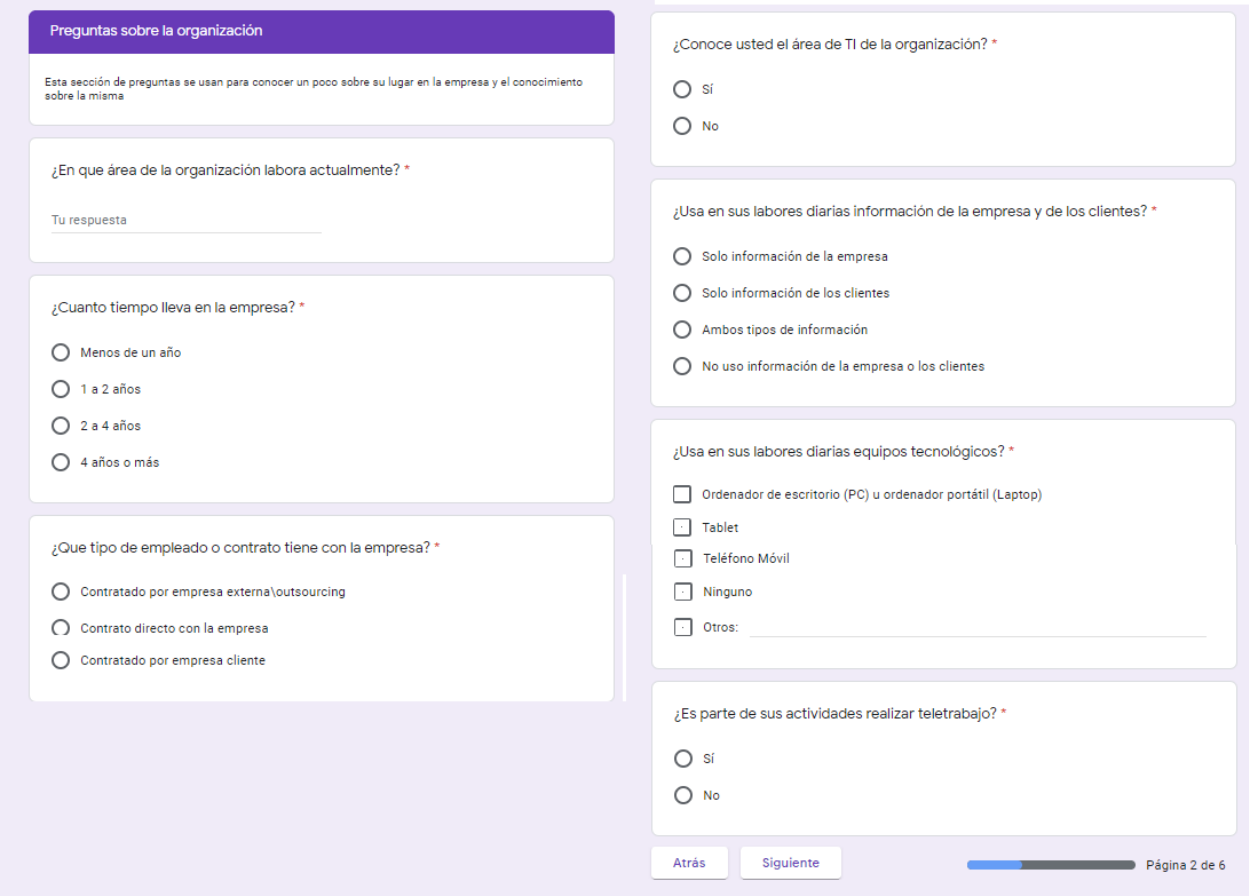
ANEXO D. ENCUESTA DE SEGURIDAD DE LA INFORMACIÓN

Figura 37. Introducción Encuesta



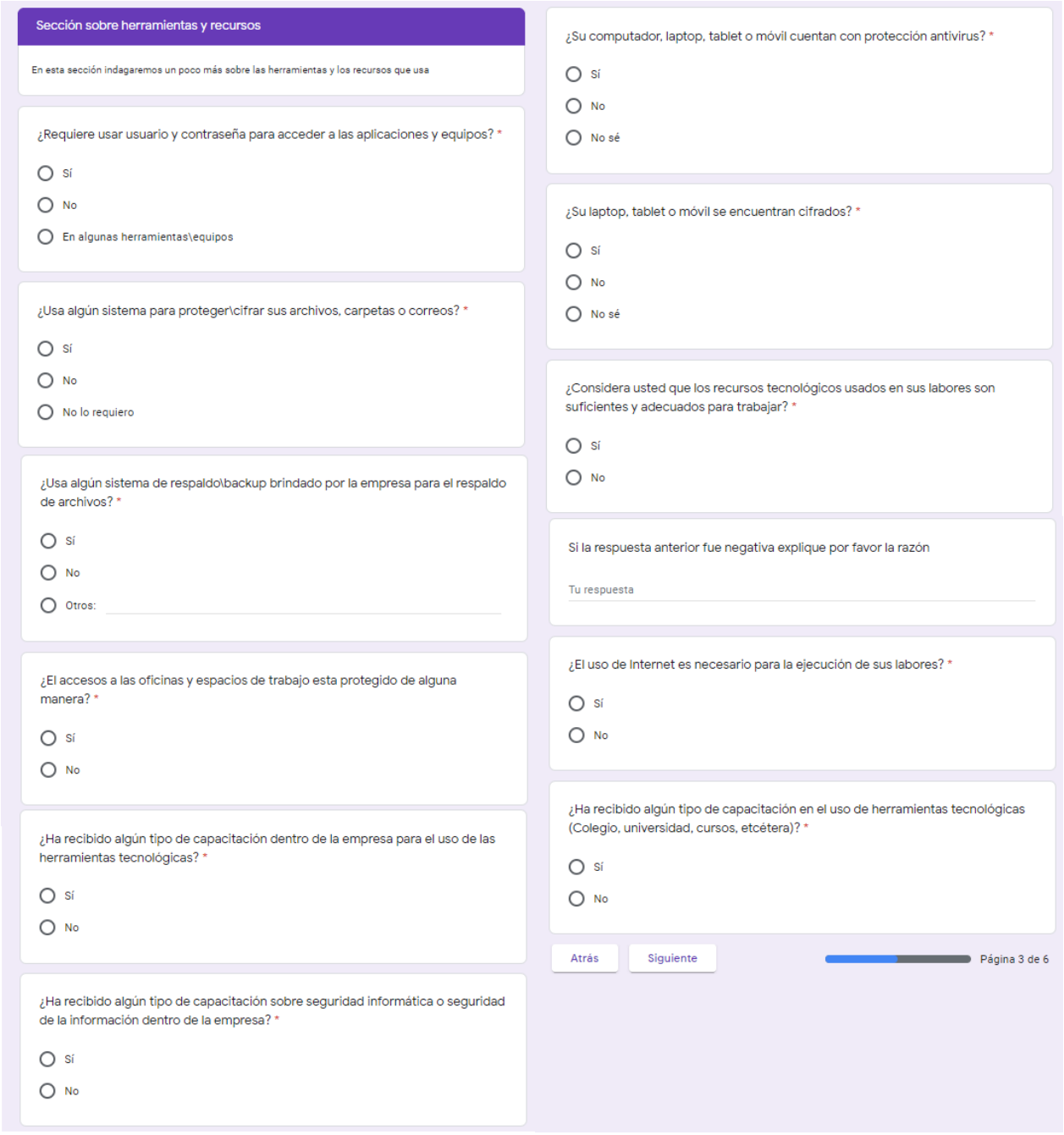
Fuente: Propia

Figura 38. Preguntas sobre la organización



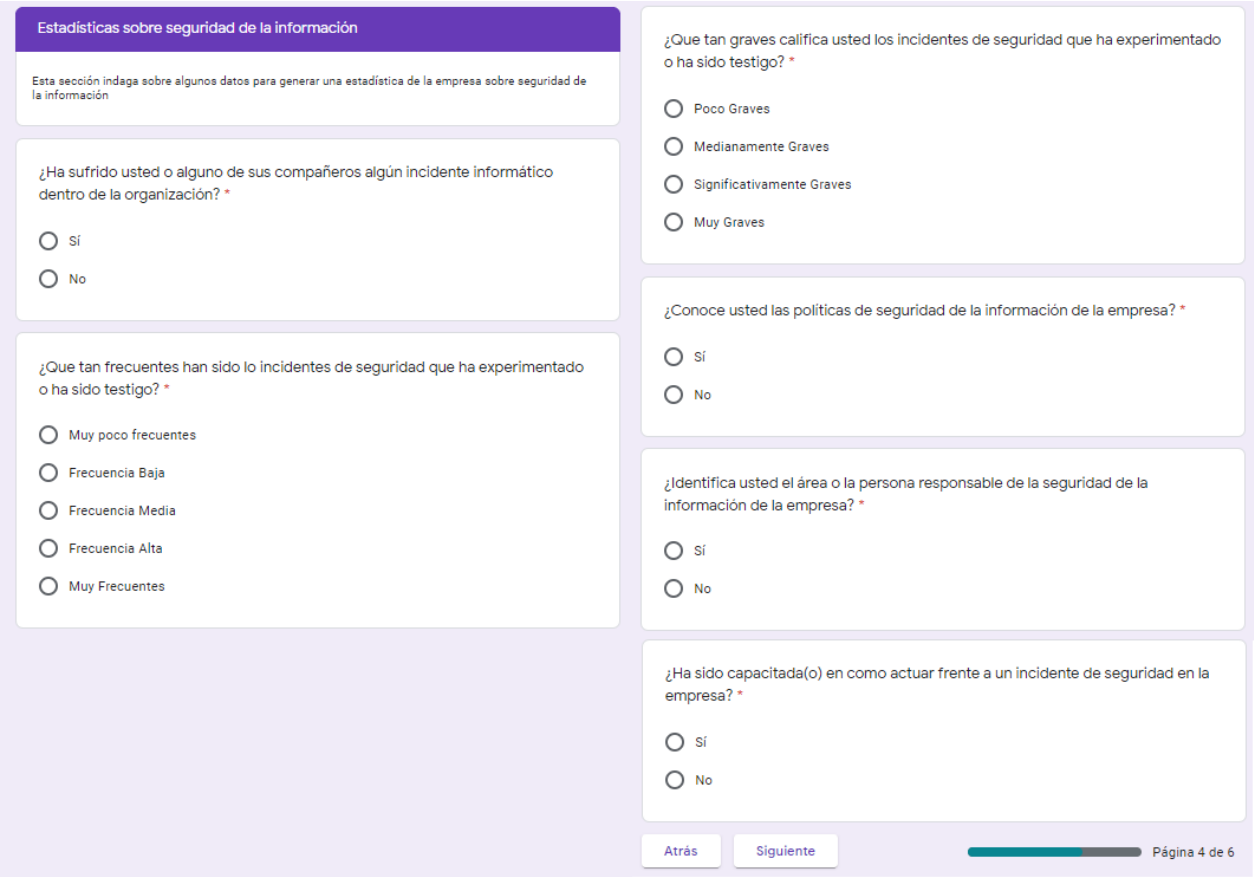
Fuente: Propia

Figura 39. Herramientas y Recursos



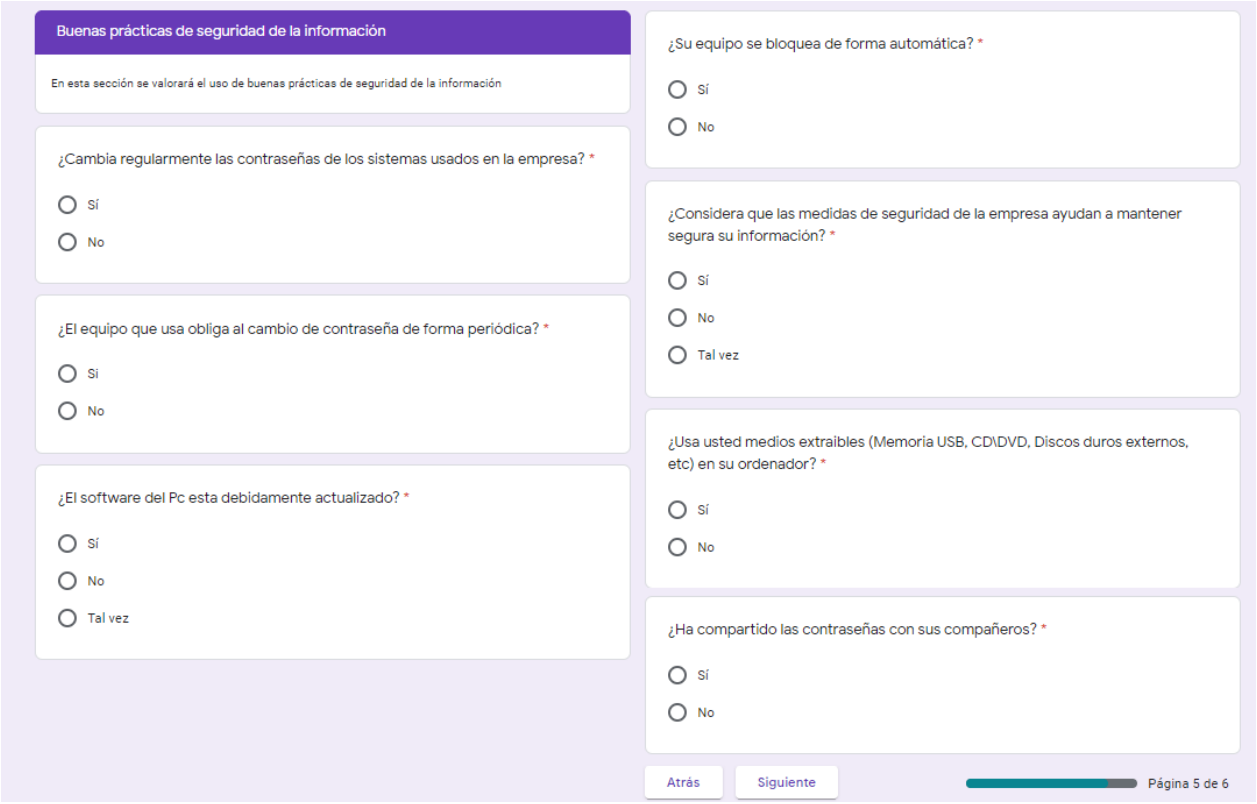
Fuente: Propia

Figura 40. Estadísticas sobre seguridad de la información



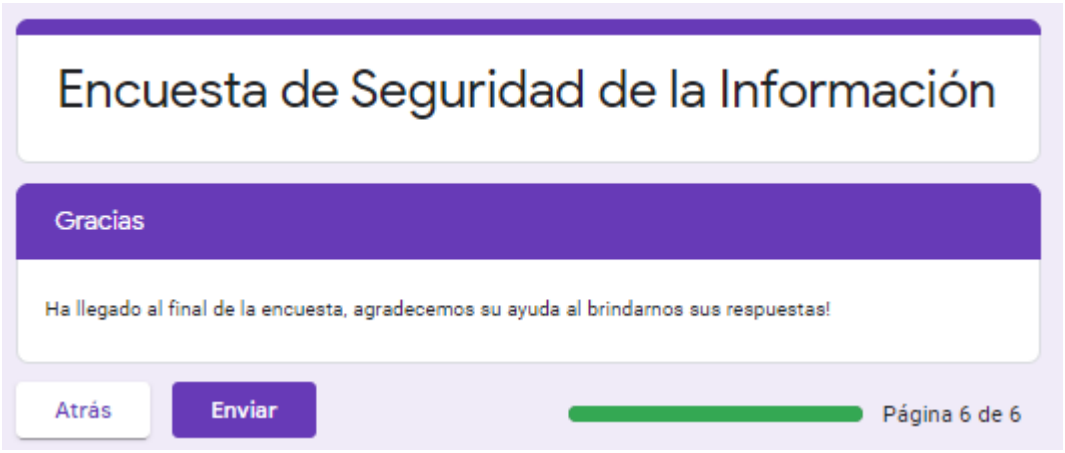
Fuente: Propia

Figura 41. Buenas prácticas de seguridad de la información



Fuente: Propia

Figura 42. Final Encuesta



Fuente: Propia

ANEXO E. RESPUESTAS ENCUESTA

Cuadro 31. Respuestas Encuesta Parte 1

PREGUNTA	RESPUESTAS				
¿En qué área de la organización labora actualmente?	TECNOLOGÍA	OPERACIONES	OPERACIONES	OPERACIONES	FORMACION
¿Cuánto tiempo lleva en la empresa?	2 a 4 años	Menos de un año	2 a 4 años	4 años o más	4 años o más
¿Qué tipo de empleado o contrato tiene con la empresa?	Contratado por empresa externa\ outsourcing	Contratado por empresa externa\ outsourcing	Contratado por empresa externa\ outsourcing	Contrato directo con la empresa	Contratado por empresa externa \outsourcing
¿Conoce usted el área de TI de la organización?	Sí	Sí	Sí	Sí	Sí
¿Usa en sus labores diarias información de la empresa y de los clientes?	Ambos tipos de información	Ambos tipos de información	Ambos tipos de información	Ambos tipos de información	Ambos tipos de información
¿Usa en sus labores diarias equipos tecnológicos?	Ordenador de escritorio (PC) u ordenador portátil (Laptop)	Ordenador de escritorio (PC) u ordenador portátil (Laptop), Teléfono Móvil	Ordenador de escritorio (PC) u ordenador portátil (Laptop), Teléfono Móvil	Ordenador de escritorio (PC) u ordenador portátil (Laptop), Teléfono Móvil	Ordenador de escritorio (PC) u ordenador portátil (Laptop)
¿Es parte de sus actividades realizar teletrabajo?	Sí	Sí	Sí	No	No
¿Requiere usar usuario y contraseña para acceder a las aplicaciones y equipos?	Sí	Sí	Sí	Sí	Sí
¿Usa algún sistema para proteger\cifrar sus archivos, carpetas o correos?	Sí	No	No	No	No

PREGUNTA	RESPUESTAS				
¿Usa algún sistema de respaldo\backup brindado por la empresa para el respaldo de archivos?	No	No	No	No	No
¿El acceso a las oficinas y espacios de trabajo está protegido de alguna manera?	No	Sí	Sí	Sí	Sí
¿Su computador, laptop, tablet o móvil cuentan con protección antivirus?	Sí	Sí	No sé	Sí	Sí
¿Su laptop, tablet o móvil se encuentran cifrados?	No	No sé	No sé	No sé	No
¿Considera usted que los recursos tecnológicos usados en sus labores son suficientes y adecuados para trabajar?	No	Sí	No	No	Sí
Si la respuesta anterior fue negativa explique por favor la razón	falta equipos de almacenamiento , para backups			Debo trabajar sobre BBDD a veces muy grandes y el computador se bloquea, a veces cierra excel y borra trabajo ya realizado	
¿El uso de Internet es necesario para la ejecución de sus labores?	Sí	Sí	Sí	Sí	Sí
¿Ha recibido algún tipo de	Sí	Sí	Sí	Sí	Sí

PREGUNTA	RESPUESTAS				
capacitación en el uso de herramientas tecnológicas (Colegio, universidad, cursos, etcétera)?					
¿Ha recibido algún tipo de capacitación dentro de la empresa para el uso de las herramientas tecnológicas?	No	No	No	No	No
¿Ha recibido algún tipo de capacitación sobre seguridad informática o seguridad de la información dentro de la empresa?	No	No	No	No	No
¿Ha sufrido usted o alguno de sus compañeros algún incidente informático dentro de la organización?	Sí	No	Sí	Sí	Sí
¿Qué tan frecuentes han sido los incidentes de seguridad que ha experimentado o ha sido testigo?	Frecuencia Media	Muy poco frecuentes	Frecuencia Media	Muy poco frecuentes	Muy poco frecuentes
¿Qué tan graves califica usted los incidentes de seguridad que ha experimentado	Muy Graves	Poco Graves	Muy Graves	Muy Graves	Significativamente Graves

PREGUNTA	RESPUESTAS				
o ha sido testigo?					
¿Conoce usted las políticas de seguridad de la información de la empresa?	Sí	No	Sí	No	Sí
¿Identifica usted el área o la persona responsable de la seguridad de la información de la empresa?	Sí	No	Sí	Sí	Sí
¿Ha sido capacitada(o) en cómo actuar frente a un incidente de seguridad en la empresa?	Sí	No	No	No	No
¿Cambia regularmente las contraseñas de los sistemas usados en la empresa?	No	Sí	Sí	Sí	Sí
¿El equipo que usa obliga al cambio de contraseña de forma periódica?	Si	Si	Si	Si	Si
¿El software del Pc está debidamente actualizado?	No	Tal vez	Tal vez	Tal vez	Tal vez
¿Su equipo se bloquea de forma automática?	No	No	Sí	No	Sí
¿Considera que las medidas de seguridad de la empresa ayudan a mantener segura su información?	Tal vez	Tal vez	No	Sí	Tal vez

PREGUNTA	RESPUESTAS				
¿Usa usted medios extraíbles (Memoria USB, CD\DVD, Discos duros externos, etc) en su ordenador?	Sí	No	No	No	No
¿Ha compartido las contraseñas con sus compañeros?	Sí	No	No	No	No

Fuente: Propia

Cuadro 32.Respuesta Parte 2

PREGUNTA	RESPUESTAS				
¿En qué área de la organización labora actualmente?	TECNOLOGÍA	OPERACIONES	OPERACIONES	CALIDAD	CALIDAD
¿Cuánto tiempo lleva en la empresa?	Menos de un año	4 años o más	4 años o más	Menos de un año	Menos de un año
¿Qué tipo de empleado o contrato tiene con la empresa?	Contratado por empresa externa\ outsourcing	Contratado por empresa externa\ outsourcing	Contrato directo con la empresa	Contratado por empresa externa\ outsourcing	Contrato directo con la empresa
¿Conoce usted el área de TI de la organización?	Sí	Sí	Sí	Sí	Sí
¿Usa en sus labores diarias información de la empresa y de los clientes?	Ambos tipos de información	Ambos tipos de información	Ambos tipos de información	Ambos tipos de información	Ambos tipos de información
¿Usa en sus labores diarias equipos tecnológicos?	Ordenador de escritorio (PC) u ordenador portátil (Laptop), Teléfono Móvil, memoria USB	Ordenador de escritorio (PC) u ordenador portátil (Laptop)	Ordenador de escritorio (PC) u ordenador portátil (Laptop), Teléfono Móvil	Ordenador de escritorio (PC) u ordenador portátil (Laptop)	Ordenador de escritorio (PC) u ordenador portátil (Laptop), Teléfono Móvil
¿Es parte de sus actividades	Sí	No	Sí	No	Sí

PREGUNTA	RESPUESTAS				
realizar teletrabajo?					
¿Requiere usar usuario y contraseña para acceder a las aplicaciones y equipos?	Sí	No	Sí	Sí	Sí
¿Usa algún sistema para proteger\cifrar sus archivos, carpetas o correos?	No	No	No	No	No
¿Usa algún sistema de respaldo\backup brindado por la empresa para el respaldo de archivos?	Sí	No	No	No	No
¿El acceso a las oficinas y espacios de trabajo está protegido de alguna manera?	Sí	Sí	No	Sí	Sí
¿Su computador, laptop, tablet o móvil cuentan con protección antivirus?	Sí	Sí	Sí	Sí	Sí
¿Su laptop, tablet o móvil se encuentran cifrados?	No	No sé	No	Sí	No sé
¿Considera usted que los recursos tecnológicos usados en sus labores son suficientes y adecuados para trabajar?	No	No	Sí	Sí	Sí
Si la respuesta anterior fue negativa explique por favor la razón	uso de accesorios y equipos personales con fines del laborales, lo	FALTA DE ENTORNOS Y BACK UP PARA FACILITAR LA GESTIÓN GENERAL.			

PREGUNTA	RESPUESTAS				
	mejor sería usar recursos directamente otorgados por la empresa.				
¿El uso de Internet es necesario para la ejecución de sus labores?	Sí	Sí	Sí	Sí	Sí
¿Ha recibido algún tipo de capacitación en el uso de herramientas tecnológicas (Colegio, universidad, cursos, etcétera)?	Sí	Sí	Sí	Sí	Sí
¿Ha recibido algún tipo de capacitación dentro de la empresa para el uso de las herramientas tecnológicas?	Sí	No	No	No	No
¿Ha recibido algún tipo de capacitación sobre seguridad informática o seguridad de la información dentro de la empresa?	No	No	No	No	Sí
¿Ha sufrido usted o alguno de sus compañeros algún incidente informático dentro de la organización?	Sí	Sí	Sí	Sí	No
¿Qué tan frecuentes han sido los incidentes de seguridad que ha experimentado o ha sido testigo?	Frecuencia Baja	Frecuencia Baja	Muy poco frecuentes	Frecuencia Baja	Muy poco frecuentes

PREGUNTA	RESPUESTAS				
¿Qué tan graves califica usted los incidentes de seguridad que ha experimentado o ha sido testigo?	Poco Graves	Muy Graves	Muy Graves	Muy Graves	Poco Graves
¿Conoce usted las políticas de seguridad de la información de la empresa?	Sí	No	Sí	No	Sí
¿Identifica usted el área o la persona responsable de la seguridad de la información de la empresa?	Sí	No	Sí	Sí	Sí
¿Ha sido capacitada(o) en cómo actuar frente a un incidente de seguridad en la empresa?	No	No	No	No	No
¿Cambia regularmente las contraseñas de los sistemas usados en la empresa?	Sí	Sí	No	Sí	Sí
¿El equipo que usa obliga al cambio de contraseña de forma periódica?	No	Si	Si	Si	Si
¿El software del Pc está debidamente actualizado?	Sí	Tal vez	No	Sí	Sí
¿Su equipo se bloquea de forma automática?	No	Sí	Sí	Sí	Sí
¿Considera que las medidas de seguridad de la empresa ayudan a mantener segura su información?	No	No	Sí	Sí	Sí
¿Usa usted medios extraíbles (Memoria USB,	Sí	No	No	No	No

PREGUNTA	RESPUESTAS				
CD\DVD, Discos duros externos, etc) en su ordenador?					
¿Ha compartido las contraseñas con sus compañeros?	No	No	No	Sí	No

Cuadro 33. Respuestas Parte3

PREGUNTA	RESPUESTAS				
¿En qué área de la organización labora actualmente?	OPERACIONES	OPERACIONES	FORMACIÓN	RRHH	BI
¿Cuánto tiempo lleva en la empresa?	Menos de un año	4 años o más	1 a 2 años	Menos de un año	Menos de un año
¿Qué tipo de empleado o contrato tiene con la empresa?	Contratado por empresa externa\outsourcing	Contrato directo con la empresa	Contrato directo con la empresa	Contrato directo con la empresa	Contrato directo con la empresa
¿Conoce usted el área de TI de la organización?	Sí	Sí	Sí	Sí	Sí
¿Usa en sus labores diarias información de la empresa y de los clientes?	Ambos tipos de información	Ambos tipos de información	Ambos tipos de información	Solo información de la empresa	Ambos tipos de información
¿Usa en sus labores diarias equipos tecnológicos?	Ordenador de escritorio (PC) u ordenador portátil (Laptop)	Ordenador de escritorio (PC) u ordenador portátil (Laptop), Teléfono Móvil	Ordenador de escritorio (PC) u ordenador portátil (Laptop)	Ordenador de escritorio (PC) u ordenador portátil (Laptop)	Ordenador de escritorio (PC) u ordenador portátil (Laptop), Teléfono Móvil
¿Es parte de sus actividades realizar teletrabajo?	No	Sí	No	Sí	No
¿Requiere usar usuario y	Sí	Sí	Sí	Sí	Sí

PREGUNTA	RESPUESTAS				
contraseña para acceder a las aplicaciones y equipos?					
¿Usa algún sistema para proteger\cifrar sus archivos, carpetas o correos?	Sí	No	No	No	No
¿Usa algún sistema de respaldo\backup brindado por la empresa para el respaldo de archivos?	No	Sí	No	No	Sí
¿El acceso a las oficinas y espacios de trabajo está protegido de alguna manera?	Sí	Sí	Sí	Sí	Sí
¿Su computador, laptop, tablet o móvil cuentan con protección antivirus?	No	Sí	Sí	No sé	Sí
¿Su laptop, tablet o móvil se encuentran cifrados?	No sé	Sí	No	No	No sé
¿Considera usted que los recursos tecnológicos usados en sus labores son suficientes y adecuados para trabajar?	No	No	Sí	Sí	Sí
Si la respuesta anterior fue negativa explique por favor la razón	Falta carpetas digitales compartidas,	No son suficientes, ya que la campaña requiere de algunas herramientas como Excel, también requiere el acceso a un			

PREGUNTA	RESPUESTAS				
		drive o un documento compartido con los agentes de la campaña, para así evitar reprocesos.			
¿El uso de Internet es necesario para la ejecución de sus labores?	Sí	Sí	Sí	Sí	Sí
¿Ha recibido algún tipo de capacitación en el uso de herramientas tecnológicas (Colegio, universidad, cursos, etcétera)?	Sí	Sí	Sí	Sí	Sí
¿Ha recibido algún tipo de capacitación dentro de la empresa para el uso de las herramientas tecnológicas?	No	No	No	No	Sí
¿Ha recibido algún tipo de capacitación sobre seguridad informática o seguridad de la información dentro de la empresa?	No	No	No	No	Sí
¿Ha sufrido usted o alguno de sus compañeros algún incidente informático dentro de la organización?	Sí	Sí	Sí	Sí	No
¿Qué tan frecuentes han sido los	Muy poco frecuentes	Frecuencia Baja	Muy poco frecuentes	Frecuencia Media	Muy poco frecuentes

PREGUNTA	RESPUESTAS				
incidentes de seguridad que ha experimentado o ha sido testigo?					
¿Qué tan graves califica usted los incidentes de seguridad que ha experimentado o ha sido testigo?	Muy Graves	Medianamente Graves	Muy Graves	Medianamente Graves	Muy Graves
¿Conoce usted las políticas de seguridad de la información de la empresa?	Sí	No	Sí	No	Sí
¿Identifica usted el área o la persona responsable de la seguridad de la información de la empresa?	Sí	Sí	Sí	No	Sí
¿Ha sido capacitada(o) en cómo actuar frente a un incidente de seguridad en la empresa?	No	No	No	No	Sí
¿Cambia regularmente las contraseñas de los sistemas usados en la empresa?	Sí	Sí	Sí	Sí	Sí
¿El equipo que usa obliga al cambio de contraseña de forma periódica?	Si	Si	Si	No	Si
¿El software del Pc está debidamente actualizado?	Sí	Tal vez	Tal vez	No	Sí
¿Su equipo se bloquea de forma automática?	Sí	Sí	Sí	No	Sí
¿Considera que las medidas de	Tal vez	Tal vez	Tal vez	No	Sí

PREGUNTA	RESPUESTAS				
seguridad de la empresa ayudan a mantener segura su información?					
¿Usa usted medios extraíbles (Memoria USB, CD\DVD, Discos duros externos, etc) en su ordenador?	No	No	No	No	No
¿Ha compartido las contraseñas con sus compañeros?	Sí	No	No	No	No

Cuadro 34. Respuestas Parte 4.

PREGUNTA	RESPUESTAS			
¿En qué área de la organización labora actualmente?	ADMINISTRACIÓN	OPERACIONES	OPERACIONES	OPERACIONES
¿Cuánto tiempo lleva en la empresa?	Menos de un año	4 años o más	1 a 2 años	Menos de un año
¿Qué tipo de empleado o contrato tiene con la empresa?	Contrato directo con la empresa	Contratado por empresa externa\outsourcing	Contrato directo con la empresa	Contrato directo con la empresa
¿Conoce usted el área de TI de la organización?	Sí	Sí	Sí	Sí
¿Usa en sus labores diarias información de la empresa y de los clientes?	Ambos tipos de información	Ambos tipos de información	Ambos tipos de información	Ambos tipos de información
¿Usa en sus labores diarias equipos tecnológicos?	Ordenador de escritorio (PC) u ordenador portátil (Laptop), Teléfono Móvil, Impresora y escaner	Ordenador de escritorio (PC) u ordenador portátil (Laptop)	Ordenador de escritorio (PC) u ordenador portátil (Laptop)	Ordenador de escritorio (PC) u ordenador portátil (Laptop), Teléfono Móvil

PREGUNTA	RESPUESTAS			
¿Es parte de sus actividades realizar teletrabajo?	No	Sí	No	Sí
¿Requiere usar usuario y contraseña para acceder a las aplicaciones y equipos?	Sí	Sí	No	Sí
¿Usa algún sistema para proteger\cifrar sus archivos, carpetas o correos?	No	No	No	No
¿Usa algún sistema de respaldo\backup brindado por la empresa para el respaldo de archivos?	Sí	No	No	No
¿El acceso a las oficinas y espacios de trabajo está protegido de alguna manera?	Sí	Sí	Sí	Sí
¿Su computador, laptop, tablet o móvil cuentan con protección antivirus?	No sé	Sí	Sí	Sí
¿Su laptop, tablet o móvil se encuentran cifrados?	No sé	Sí	No	No sé
¿Considera usted que los recursos tecnológicos usados en sus labores son suficientes y adecuados para trabajar?	Sí	Sí	No	No
Si la respuesta anterior fue negativa explique por favor la razón			su procesador no es suficiente para las aplicaciones y funciones de mi	Falta recursos en los equipos actuales, RAM, procesador

PREGUNTA	RESPUESTAS			
			cargo. siempre se queda pegado ocasionando reprocesos y tiempos de gestión perdidos.	
¿El uso de Internet es necesario para la ejecución de sus labores?	Sí	Sí	Sí	Sí
¿Ha recibido algún tipo de capacitación en el uso de herramientas tecnológicas (Colegio, universidad, cursos, etcétera)?	Sí	Sí	Sí	Sí
¿Ha recibido algún tipo de capacitación dentro de la empresa para el uso de las herramientas tecnológicas?	No	Sí	Sí	No
¿Ha recibido algún tipo de capacitación sobre seguridad informática o seguridad de la información dentro de la empresa?	No	No	No	No
¿Ha sufrido usted o alguno de sus compañeros algún incidente informático dentro de la organización?	Sí	Sí	Sí	Sí
¿Qué tan frecuentes han sido lo incidentes de seguridad que ha experimentado o ha sido testigo?	Muy poco frecuentes	Muy poco frecuentes	Frecuencia Baja	Frecuencia Baja

PREGUNTA	RESPUESTAS			
¿Qué tan graves califica usted los incidentes de seguridad que ha experimentado o ha sido testigo?	Muy Graves	Muy Graves	Significativamente Graves	Muy Graves
¿Conoce usted las políticas de seguridad de la información de la empresa?	No	Sí	Sí	Sí
¿Identifica usted el área o la persona responsable de la seguridad de la información de la empresa?	Sí	Sí	Sí	Sí
¿Ha sido capacitada(o) en cómo actuar frente a un incidente de seguridad en la empresa?	No	No	No	No
¿Cambia regularmente las contraseñas de los sistemas usados en la empresa?	No	Sí	Sí	Sí
¿El equipo que usa obliga al cambio de contraseña de forma periódica?	No	Si	Si	Si
¿El software del Pc está debidamente actualizado?	Sí	Sí	Sí	Sí
¿Su equipo se bloquea de forma automática?	Sí	Sí	Sí	Sí
¿Considera que las medidas de seguridad de la empresa ayudan a mantener segura su información?	Tal vez	Tal vez	Tal vez	Sí

PREGUNTA	RESPUESTAS			
¿Usa usted medios extraíbles (Memoria USB, CD\DVD, Discos duros externos, ¿etc) en su ordenador?	No	No	No	No
¿Ha compartido las contraseñas con sus compañeros?	Sí	No	No	No

Fuente: Propia

ANEXO F. ACEPTACIÓN EMPRESA

Figura 43. Carta aceptación de la empresa

Pereira, Abril 06 de 2018

Señores
Universidad Nacional Abierta y a Distancia – UNAD
Ciudad

Cordial saludo,

La presente para informar que el Sr. Germán Andrés Olano Trejos, Estudiante de la Especialización en Seguridad Informática de la Universidad Nacional Abierta y a Distancia (UNAD), se le ha autorizado para realizar un proceso de análisis enfocado en el Sistema de Gestión de Seguridad de la Información dentro de nuestra empresa, lo anterior como parte del ejercicio pedagógico para optar al título de especialista.

Agradecemos la atención brindada.

Cordialmente,

JAVIER ANDRES GUTIERREZ
Representante Legal