Plan de Seguridad Informática

Diego Alberto Duque Agudelo

Trabajo de grado presentado para optar al título de Ingeniero de Sistemas

Asesora

Sandra Patricia Zabala Orrego, Especialista (Esp) en Gerencia de Proyectos

Universidad de Antioquia

Facultad de Ingeniería

Ingeniería de Sistemas

Medellín, Antioquia, Colombia

2022

Dedicatoria

A mi persona, por resistir en aquellas noches largas en las que la frustración y el cansancio parecería opacar mi sueño de ser ingeniero de la Universidad de Antioquia, por entender que algunas derrotas hacen parte del proceso y que más pronto que tarde vería los resultados, por sacrificar momentos maravillosos con mis seres amados para cumplir con mis compromisos académicos, por aquellos días en que lloré por no obtener los resultados esperados, por comprender que la educación vale mucho más que el dinero, por aquellos días en que aún teniendo el corazón roto continué adelante, por los ocasos que nunca disfruté y por las albas que contemplé al frente del computador.

A mí madre Luz Dary Agudelo y padre Rodrigo Duque, por siempre creer en mi y brindarme sus palabras de aliento cuando las necesité, a mis 9 hermanos por siempre estar para mi y brindarme su apoyo incondicional, a mis abuelos fallecidos por sus miradas enternecidas y por siempre expresarme su orgullo, a mi perrita Lulú que con su partida se llevó mi corazón y a Lucas que ha sabido llenar su vacío.

A todas aquellas personas que he conocido en mi vida y que han dejado una hermosa huella demostrándome que el mundo no es tan malo porque en él están ellas.

Agradecimientos

A la gloriosa Universidad de Antioquia por abrirme las puertas de su alma máter, por ser mi hogar durante todos estos años, por enseñarme que debemos luchar por un mundo mas justo para todos sin importar los privilegios que tengamos, le agradezco especialmente, por ser de los mejores lugares que he conocido y que conoceré en mi vida.

También quiero agradecer a los profesores que son su sabiduría y temple me guío durante toda la carrera, a los profesionales y compañeros que han aportado a mis conocimientos.

Finalmente quiero agradecer a mi familia por todo su apoyo, amor y comprensión, porque sin ellos nunca lo hubiera podido lograr.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

SIGLAS, ACRÓNIMOS Y ABREVIATURAS

RRHH.	Recursos Humanos
CCTV.	Circuito Cerrado Televisión
WAF.	Web Application Firewall
IPS.	Intrusion Prevention System
IDS.	Intrusion Detection System
VLAN.	Virtual Local Address Network
PSI.	Plan de Seguridad Informática
UPS.	Uninterruptible Power Supply
UTP.	Unshielded Twisted Pair
OSI.	Open System Interconnection
MPLS.	Multiprotocol Label Switching
LAN.	Local Address Network
SDWAN.	Secure Define Wide Area Network
VPN.	Virtual Private Network
SSL.	Secure Sockets Layer
RTO.	Recovery Time Objetive
RPO.	Recovery Point Objetive

RESUMEN

La norma ISO-IEC 27001 debe ser entendida como un conjunto de buenas prácticas para la seguridad de la información, desarrollado desde la experiencia de la implementación de controles para la seguridad de la información aceptados por las empresas y organizaciones más importantes del mundo; por ello, Socia BPO entendiendo la necesidad de protección de su información y la de sus clientes, ha decidido implementar este conjunto de buenas prácticas para alinear su operación con estándares internacionales que garanticen disponibilidad, confidencialidad e integridad de sus activos más críticos.

El presente proyecto pretende dar a conocer la importancia de implementar un Plan de Seguridad Informática en las empresas que garantice que la información está siendo gestionada por los colaboradores de forma segura y que los riesgos son identificados, gestionados y mitigados de forma proactiva para prevenir que las amenazas se materialicen.

Finalmente, este proyecto espera que la empresa cuente con un proceso de seguridad de la información maduro que brinde tranquilidad y felicidad a sus directivos y clientes, también, que apalanque de forma óptima y segura los proyectos actuales y futuros dando valor a la organización en todos sus procesos misionales.

Palabras clave **— SGSI, ISO-IEC 27001, Estándar de Seguridad, buenas prácticas de seguridad.**

ABSTRACT

ISO-IEC 27001 must be understood as a set of good practices for the security of the information, developed from the experience of implementing controls for it that are accepted by the most important companies in the world; For that, Socia BPO understanding the need of protecting their's and client's information, has decided to implement this set of good practices to align their operation with international standars that can guarantee the availability, confidentiality and integrity of their most critical assets.

This project pretends to get to know the importance of implementing an IT Security Plan in the Companies to guarantee that the information it being managed safely by the employees, risks and threats can be identified, managed, and solved proactively to prevent them from materializing.

Finally, this project expects that the Company counts with a process of Security of the information that can offer tranquility and happiness to their directors and clients, also that optimally and safely leverages current projects and future giving value to the organization in all its mission processes.

Keywords — **ISMS, ISO-IEC 27001, security standard, good security practices.**

I. INTRODUCCIÓN

Socia BPO S.A.S es una organización que presta servicios BPO a un grupo empresarial automotriz, conformado por 14 empresas (inclusive). Los servicios se prestan de forma transversal a cada una de estas, respetando su individualidad de marca; buscando optimizar los recursos y ofrecer un servicio de alta calidad.

Las áreas que conforman Socia BPO son: tecnología informática, recursos humanos, seguridad y vigilancia, contraloría y vinculación y compensación.

Socia BPO fue fundada en el 2014 y actualmente cuenta con 40 colaboradores que trabajan cada día con entusiasmo, bajo una cultura de felicidad y realización personal, que se convierte en una satisfacción con un porcentaje por encima del 95% en la prestación de servicios a sus clientes.

En su afán por brindar un excelente servicio Socia BPO ha decidido implementar un Plan de Seguridad Informática que sea transversal a las organizaciones. Este, con el fin de garantizar que cada uno de los procesos están respaldados por buenas prácticas de seguridad de la información y que brinde tranquilidad a sus directivos, empleados y clientes en sus operaciones.

Socia BPO, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el estado, los ciudadanos y clientes, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

II. PLANTEAMIENTO DEL PROBLEMA

Para Socia BPO, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados.

Para iniciar con la ejecución del proyecto, es indispensable realizar un mapa del estado actual de la organización con respecto al cumplimiento de la norma ISO-IEC 27001, esto se puede realizar mediante un análisis GAP que no es más que un método para evaluar las diferencias entre el estado actual de seguridad de la información (donde estamos ahora) y el estado objetivo al que espera llegar esta (donde queremos estar). [1]

El análisis GAP se realiza a la organización basando en los 14 dominios que hacen parte de la norma ISO-IEC 27001, este debe brindar conclusiones cualitativas que proporcionen información más precisa frente a los hallazgos.

A. Antecedentes

El análisis GAP fue realizado en la organización mediante cuestionarios y entrevistas a los responsables de cada uno de los procesos, estos resultados se cuantifican y se da un valor de cumplimento basado en la norma ISO-IEC 27001.

Podemos resumir los hallazgos en tres grupos: Controles de Gestión, Controles Técnicos y Controles Operativos.

En los Controles de Gestión se tienen 4 dominios: Políticas de Seguridad, Organización de la Información, Cumplimiento y Seguridad de los RRHH.

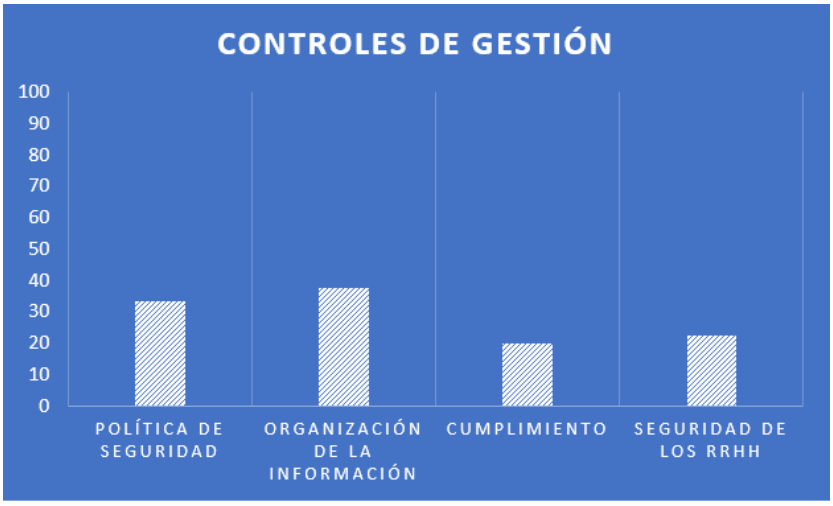

Fig. 1. Controles de Gestión.

En cuanto a las Políticas de Seguridad se identifica que la organización cuenta con algunas políticas básicas, sin embargo, estas no están completamente documentadas, no cuentan con procedimientos que las apoyen y no existen controles que garanticen la efectividad de la aplicación de las políticas.

Fig. 2. Políticas de seguridad – GAP.

Para la Organización de la Información, la empresa no cuenta con controles adecuados que permita un acceso seguro a la información por parte de terceros, clientes y usuarios, así mismo, no existen acuerdos de confidencialidad que garanticen la custodia y la confidencialidad de la información.

Fig. 3. Organización de la Información – GAP.

El dominio de Cumplimiento de la organización es bajo ya que nunca han tenido auditorías externas que permitan conocer el estado actual de la seguridad de los activos por terceros, sin embargo, la empresa cada año realiza auditorías internas y las no conformidades son corregidas.

Fig. 4. Cumplimiento – GAP.

La Seguridad de los RRHH se encuentra establecida pero no dentro del marco de la norma, por lo que es necesario implantar en la inducción y reinducción la seguridad de la

información y la importancia que tiene para la organización, todos los colaboradores deben conocer la política de seguridad y tener fácil acceso a esta.

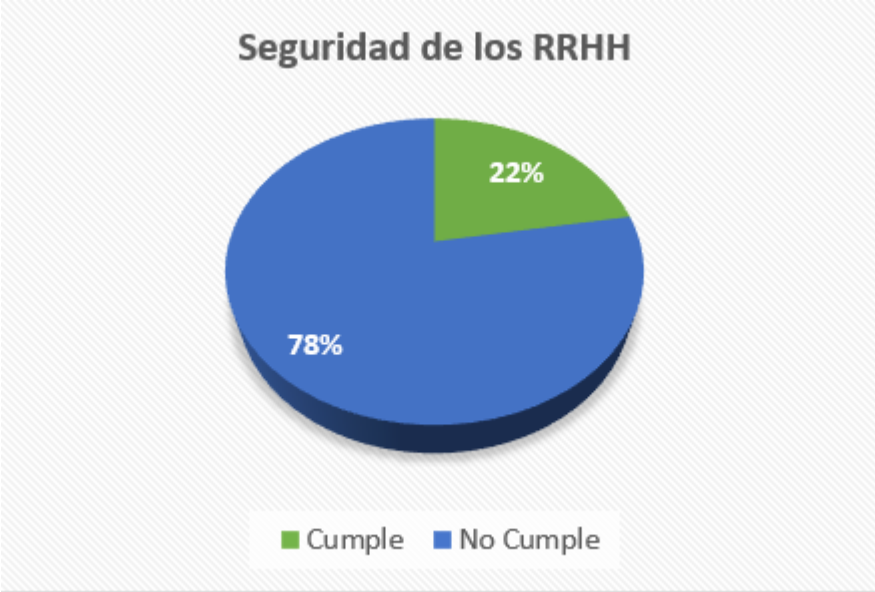

Fig. 5. Seguridad de los RRHH – GAP.

En los Controles Técnicos se tienen 3 dominios: Gestión de Activos, Gestión Física y del Ambiente y Gestión de Comunicaciones y Operaciones.

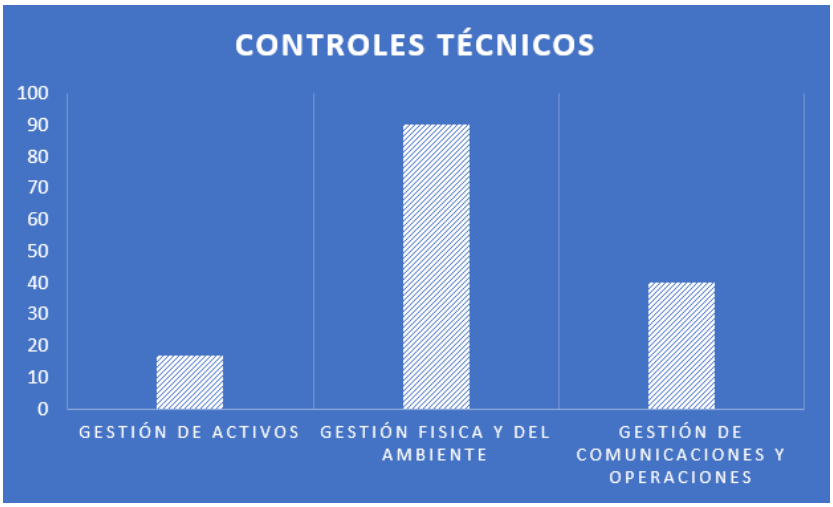

Fig. 6. Controles Técnicos.

Para el control de Gestión de Activos, se debe reforzar la clasificación y la etiquetación de activos de acuerdo con su criticidad, ya que esto es fundamental para priorizar los controles que se le deben aplicar a los que tengan una criticidad alta para la organización.

Fig. 7. Gestión de Activos – GAP.

De los controles más completos en la organización es la Gestión Física y del Ambiente, pues los centros de datos cuentan con controles de acceso y estos cuentan con una correcta climatización y contingencia frente a problemas de energía para los equipos de cómputo, sin embargo, es necesario mejorar la documentación de acceso y trabajos en los centros de datos ya sea para personal interno o para proveedores que realicen actividades en estos espacios; la organización cuenta con personal de Vigilancia y Seguridad y CCTV en toda la sede que protege los activos frente a problemas de seguridad locativos.

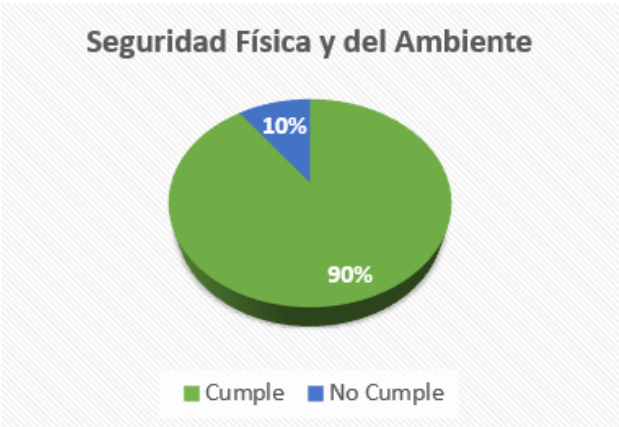

Fig. 8. Seguridad Física y del Ambiente – GAP.

Para el dominio de Gestión de Comunicaciones y Operaciones se detalla que los servidores se encuentran alojados en un datacenter de Claro (Triara), estos son los encargados de garantizar la disponibilidad del sistema, esto también aplica a asignación de recursos adicionales en el caso de ser necesarios, así mismo, este proveedor es el responsable de realizar las copias de seguridad de todos los servicios que se encuentran alojados allí.

A nivel de usuario se está implementando un sistema antivirus con el cual se busca proteger a los usuarios de los diferentes ataques informáticos de los que puedan ser víctimas, así como una reparación de las vulnerabilidades que se alojan en los puntos finales.

El entorno de producción y de desarrollo se encuentra separado, se debe considerar madurar con documentación más clara sobre quién, y cuándo se ingresa a la información.

Las redes se encuentran segmentadas por VLAN a nivel local, a nivel general de la red se encuentra protegida por Firewalls, WAF, IDS/IPS y SDWAN.

El proceso no tiene documentado los procedimientos operativos que se realizan, también se debe estandarizar un control de cambios en el cual se deje evidencia las operaciones realizadas y el motivo, esto incluye actualizaciones y lanzamiento de nuevas versiones.

Socia BPO no cuenta con un plan de respuesta frente a un incidente de seguridad que pueda poner en peligro la confidencialidad, integridad y disponibilidad de los recursos de producción del sistema, este documento debe describir de forma general, cómo actuar frente a una situación de esta magnitud para ofrecer una respuesta ágil y eficiente.

Por política de la empresa no se bloquea el acceso de medios extraíbles como USB, CD’s e impresiones de documentos, si esto no se desea regular, debe agregarse a la política general de uso de los sistemas informáticos.

Se debe reforzar el cifrado en tránsito para proteger la integridad y confidencialidad de la información, especialmente para los sistemas de transacciones en línea que transiten por la red, así mismo se debe minimizar lo máximo posible la superficie de ataque.

Fig. 9. Gestión de Comunicaciones y Operaciones – GAP.

En los Controles de Gestión se tienen 4 dominios: Adquisición Desarrollo y Mantenimiento de Sistemas, Control de Acceso, Gestión de Incidentes y Continuidad del Negocio.

Fig. 10. Controles Operacionales.

En el Control de Adquisición Desarrollo y Mantenimiento de Sistemas no se encuentra una estandarización de los procesos de desarrollo, despliegue, testeo y mantenimiento, los sistemas son liberados por demanda sin ninguna prueba de seguridad posterior, por lo que se deben crear los procedimientos que estandarice todo el ciclo de desarrollo y que las aplicaciones y/o sistemas sean seguras para la organización cuando se encuentren en producción.

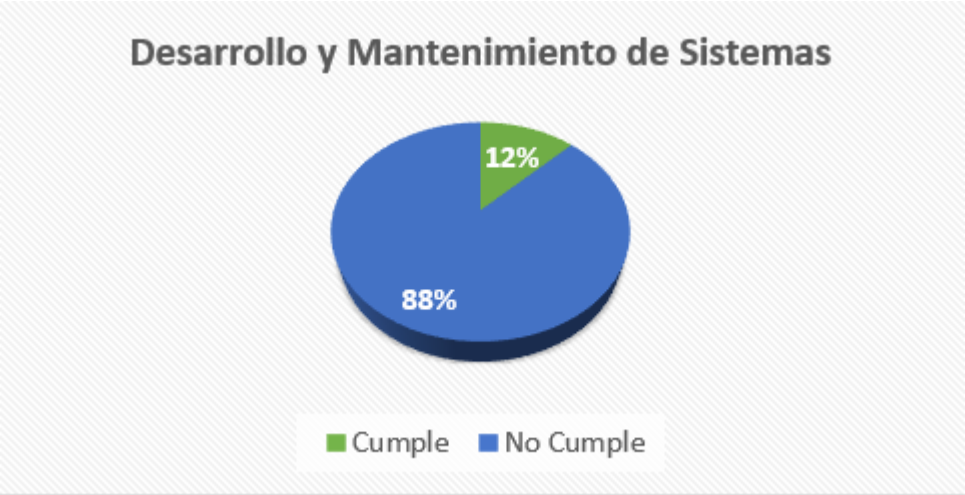

Fig. 11. Desarrollo y Mantenimiento de Sistemas – GAP.

Para el Control de Acceso se encuentra que la autenticación está centralizada por el directorio activo y las contraseñas se deben cambiar cada 42 días, así mismo estas están regidas por políticas de complejidad y bloqueo automático del PC después de un tiempo de inactividad.

Actualmente existe una política de uso de los servicios informáticos, pero esta debe actualizarse de acuerdo con las necesidades del proceso y del negocio.

Se deben crear políticas que definan claramente los controles de acceso y los perfiles de los usuarios dentro de compañía, pues actualmente muchos accesos se dan por defecto o sin una justificación de uso.

Es importante documentar el procedimiento que se realiza en las bajas y altas de los usuarios, adicionalmente se debe documentar el protocolo de teletrabajo, esto con respecto a los accesos y la seguridad de los puntos finales.

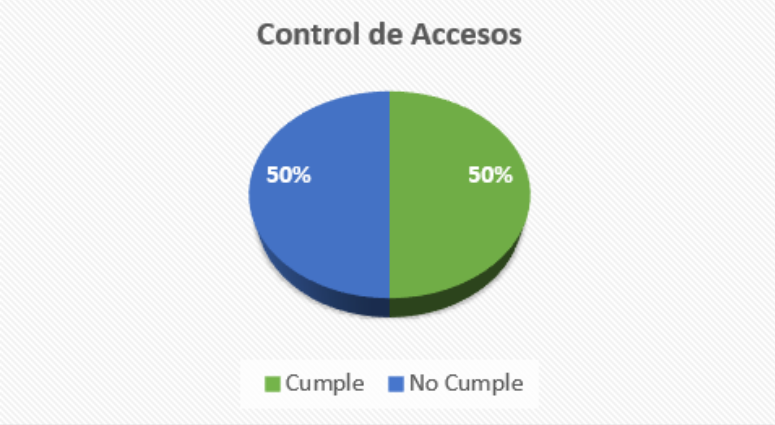

Fig. 12. Control de Acceso – GAP.

Socia BPO actualmente no cuenta con controles de Gestión de Incidentes, pues este se realiza de forma reactiva, el proceso debe llevar a un nivel de madurez donde se actúe de forma preventiva frente a los posibles eventos de seguridad que se puedan presentar.

Fig. 13. Gestión de Incidentes – GAP.

La Gestión de Continuidad del Negocio tampoco cuenta con controles establecidos, actualmente la única forma de recuperar la operación del negocio es mediante sistemas de Backup, los cuales pueden tener un tiempo de recuperación muy alto y producir pérdidas grandes en la productividad de la organización.

Fig. 14. Gestión de Continuidad del Negocio – GAP.

A nivel general podemos concluir que el nivel de madurez en seguridad informática de Socia BPO se encuentra en un 41%, el cual pertenece a las políticas de seguridad aplicadas actualmente, estás si bien son efectivas deben ser reforzadas, documentadas, comunicadas y reglamentadas para que sean de cumplimiento general en la organización, también se considera en este nivel de madurez la preparación y esfuerzos realizados por Socia BPO en prepararse para la implementación del PSI, entre estos se encuentra la contratación del personal, la disposición de la coordinación y equipo de TI y la voluntad de la alta gerencia para apoyar el proceso.

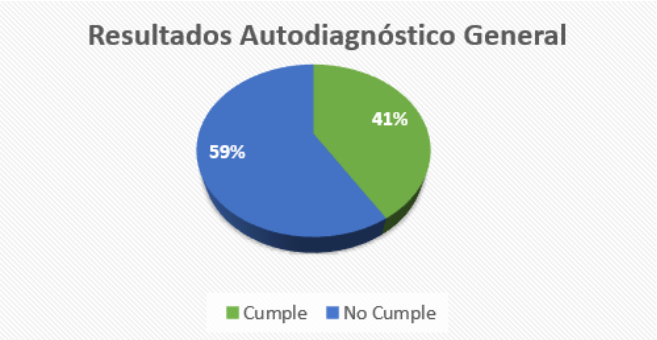

Fig. 15. Resultados Autodiagnóstico General.

III. OBJETIVOS

A. Objetivo general

Diseñar políticas, procedimientos y controles de seguridad de la información basadas en buenas prácticas internacionales, con el fin de realizar una gestión segura de los activos informáticos en cada uno de los procesos transversales de la organización.

B. Objetivos específicos

- Diseñar las políticas recomendadas por la norma ISO-IEC 27001.
- Diseñar los procedimientos recomendados por la norma ISO-IEC 27001.
- Ejecutar los controles recomendados por la norma ISO-IEC 27001.
- Realizar la matriz de riesgos a los que está expuesta la organización.
- Crear las estrategias de tratamiento de riesgos identificados.

IV. MARCO TEÓRICO

La norma técnica ISO-IEC 27001 fue publicada por primera vez en octubre del 2005 por la Organización Internacional de Estandarización (ISO) y por la Comisión Electrónica Internacional (IEC). Su función es garantizar que las organizaciones garanticen una mejora continua y una administración adecuada de la información [2], esta norma es considerada un estándar de talla internacional. Si bien no es aún obligatorio su cumplimiento, cada vez es más solicitada por las empresas, principalmente cuando buscan relaciones comerciales o disposiciones legales, pues, la implantación de esta norma es garantía de prácticas saludables al interior de la organización que garantizan la confidencialidad, integridad y disponibilidad de la información; dando tranquilidad a sus clientes y socios de negocio.

El interés por gestionar la seguridad de la información surgió por los riesgos a los que se está en un mundo cada vez más digitalizado, por ello, es necesario contar con controles que garanticen que uno de los activos más importantes para las empresas (la información) sea

protegido y custodiado de forma eficiente. El Economista de México informa que durante el año 2021 las empresas tuvieron pérdidas por 8 mil millones de dólares a nivel global [3], según el periódico El Mundo el 60% de estas empresas tuvo que cerrar su operación por las pérdidas ocasionadas por los ciberataques y la mayoría de estas pertenecía a la categoría PYME [4]. Estás pequeñas empresas normalmente son las más golpeadas ya que al carecer de controles y/o personal experto en seguridad informática los ataques son mucho más contundentes.

Si bien, en seguridad de la información nunca podemos hablar de una mitigación total del riesgo, la implementación de políticas de seguridad en la organización disminuye notablemente de que las amenazas sean materializadas, la norma aborda aspectos importantes que refuerzan el uso seguro de los sistemas de información, por ejemplo, la norma requiere un compromiso por parte de los directivos (los cuales son los menos preocupados por la seguridad de la organización, principalmente por considerarlos un gasto) que debe garantizar que existan los recursos para su implantación y que el cumplimiento y capacitación del personal estará impulsado por estos, de igual forma, deberán estructurar el proyecto y definir el alcance que se requiere en el negocio, aunque este es un estándar, no es aplicable totalmente a todas las empresas, por lo que, este debe alinearse con la visión y misión del negocio y darle valor.

La norma garantiza que los procesos misionales se encuentran estandarizados y asegura que funcionan correctamente dentro del sistema de seguridad, también, gestiona los riesgos basados en la clasificación dada, por ejemplo, en riesgos críticos, alto, medios y bajos, donde los críticos y altos tienen una prioridad especial de gestión.

Finalmente, la implantación de la norma permite una mejora continua con procesos metódicos; esto permite establecer cuáles son los factores por mejorar para que aumente la productividad y para conocer cuál metodología es útil a la hora de evaluar el rendimiento del trabajo y detectar aspectos que se deben perfeccionar. [2]

V. METODOLOGÍA

El Plan de Seguridad, ha creado un comité conformado por 3 integrantes (Líder Seguridad Informática, Dirección Tecnología Informática y Gerencia) su función es revisar la aplicabilidad de las políticas y ajustar éstas a la cultura organizacional, luego, cuando son aprobados los documentos pasan a un repositorio general en formato PDF con su respectiva fecha de emisión. Finalmente, pasan a su etapa de implementación en toda la organización, esto requiere de sensibilización y capacitación para el personal interesado.

Los procedimientos se crean en conjunto con el comité técnico que está conformado por los líderes de procesos (Soporte, Operaciones, Telecomunicaciones, Seguridad y Dirección) donde cada uno como responsable de proceso se debe encargar de construir sus procedimientos, los cuales son solicitados y apoyados por el Líder de Seguridad Informática para que permanezcan dentro del marco de la norma.

Los controles son construidos por el Líder de Seguridad Informática, estos deben ser aprobados y apoyados por la dirección de tecnología y la gerencia, cada uno de estos controles son auditados de acuerdo con la periodicidad establecida en las políticas, la auditoría puede ser realizada tanto por personal interno como por auditores externos.

La matriz de riesgos es creada por el Líder de Seguridad Informática y socializada con los líderes de cada uno de los procesos y con quien corresponda dentro de la organización. En el comité técnico se definen las estrategias de tratamiento de riesgos.

La metodología para operar la gestión documental es la siguiente:

- Las políticas se tipifican de la siguiente manera: PL = Política - IN = Infraestructura + Consecutivo
- Los procedimientos se tipifican: PR = Procedimiento - IN = Infraestructura + Consecutivo
- Los controles se tipifican como formatos que deben ser diligenciados, FT = Formato - IN = Infraestructura + Consecutivo

- Todos los documentos se referencian en un listado maestro, que permite visualizar de forma clara cada uno de los documentos con su respectivo consecutivo, además, tiene detallada de forma clara dónde se almacena la información y en qué forma se debe hacer.
- Todos los documentos cuentan con control de versionamiento, el cual debe contar con la fecha de creación del documento, versión, quién lo crea, quién lo revisa y quién lo aprueba. Adicional a esto, tiene una fecha de emisión que corresponde a la fecha de aprobación de la política, procedimiento o control.
- Toda la información es guardada en SharePoint tanto en su versión editable como en su versión publicada en PDF.

VI RESULTADOS

En el desarrollo del Plan de Seguridad Informática de establecen las políticas, procedimientos y controles recomendados por la norma ISO-IEC 27001 con sus 14 dominios, los cuales buscan estandarizar las operaciones de la organización de tal manera que esta pueda garantizar los tres pilares fundamentales de la seguridad de la Información CIA (Confidencialidad, Integridad y Disponibilidad) en todos sus procesos.

Los riesgos identificados en el análisis GAP, en su mayoría ya fueron mitigados con las políticas, procedimientos y controles definidos en el Plan de Seguridad Informática.

A continuación, se realizará un recorrido por cada uno de los documentos creados para tal fin, alguna información se omitirá de forma voluntaria ya que podría violar la confidencialidad de la organización.

1. Política General

Inicialmente se define la Política General la cuál no es más que el establecimiento del Plan de Seguridad Informática y que concreta los objetivos del Plan de Seguridad de la Información, principios de seguridad de la información, indicadores clave, nivel de cumplimiento y políticas que se desarrollarán para la organización.

1.1 Objetivos del Plan de Seguridad de la Información

- Comprender y tratar los riesgos operacionales y estratégicos en seguridad de la información para que permanezcan en niveles aceptables para la organización.
- Proteger la información confidencial relacionada con los clientes, terceros, planes de desarrollo y finanzas corporativas.
- La conservación de la integridad de los sistemas de información y de los registros contables.
- Mantener la disponibilidad de los servicios indispensables, para soportar la operación del negocio.
- Proteger los servicios WEB y las redes internas con las mejores prácticas de seguridad.
- Entender y dar cobertura a las necesidades de cada uno de los procesos del negocio, implementando mejoras en seguridad que permitan dar tranquilidad a la operación.

1.2 Principios de Seguridad de la Información

- La organización afronta la toma de riesgos y tolera aquellos que, con base en la información disponible, son comprensibles, controlados y tratados cuando es necesario.
- Todo el personal será informado y responsable de la seguridad de la información, según sea relevante para el desempeño de su trabajo.
- Se dispondrá de financiación para la gestión operativa de los controles relacionados con la seguridad de la información y en los procesos de gestión para su implantación y mantenimiento.
- Los riesgos en seguridad de la información serán objeto de seguimiento y se adoptarán medidas relevantes cuando existan cambios que impliquen un nivel de riesgo no aceptable.
- Los criterios para la clasificación y la aceptación del riesgo se encuentran referenciados en la política.
- Las situaciones que puedan exponer a la organización a la violación de las leyes y normas legales no serán toleradas.
- Mantener la confianza de sus clientes, socios, empleados y cualquier tercero con el que se establezca alguna relación.
- Apoyar la innovación tecnológica.

- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los directivos, gerentes, funcionarios, y terceros.

1.3 Indicadores Clave

- Incidentes de seguridad de la información por año
- Análisis de Seguridad interno/externo por año
- Disponibilidad de los servicios indispensables para la operación por encima del 99%
- Sensibilización a los colaboradores, directivos y personal de TI, 2 veces por año
- Cumplimiento de los objetivos del Plan de Seguridad establecidos para el año en curso

1.4 Políticas relacionadas

Se detallan las políticas que proporcionan principios y guía en aspectos específicos de Seguridad de la Información:

PLIN002 - Uso adecuado de activos
PLIN003 - Intercambio de información con terceros
PLIN005 - Gestión de contraseñas
PLIN006 - Gestión de activos de información
PLIN007 - Ingreso de proveedores
PLIN009 - Control de acceso
PLIN010 - Seguridad de operaciones
PLIN011 - Relación con proveedores
PLIN012 - Seguridad de comunicaciones
PLIN013 - Controles criptográficos
PLIN014 - Capacitación y sensibilización
PLIN015 - Auditoría de actividades de seguridad TI
PLIN016 - Seguridad física y del entorno

Políticas dirigidas directamente a los usuarios:

PLIN002 - Uso del Internet
PLIN002 - Uso del correo y mensajería instantánea
PLIN002 - Responsabilidades de los colaboradores con la seguridad de la información
PLIN002 - Uso de portátiles y dispositivos móviles
PLIN002 - Seguridad en el puesto de trabajo
PLIN002 - Daños a cargo del colaborador

PLIN009 - Política de escritorio limpio
PLIN010 - Protección contra software malicioso
PLIN002 - Instalación de Software ilegal
PLIN008 - Política de uso de celulares corporativos

1.5 Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento al 100% a esta política de Seguridad de la Información.

1.6 Asignación interlocutores ISO-IEC 27001

Los interlocutores presentados en la TABLA 1 son aquellos responsables por aportar información valiosa para adaptar el Plan de Seguridad Informática a la naturaleza de sus procesos.

TABLA I
ASIGNACIÓN INTERLOCUTORES

CONTROLES	INTERLOCUTORES
A.5 Políticas de Seguridad de la Información	**Infraestructura TI**
A.6 Organización de la Seguridad de la Información	**Director Infraestructura TI + Líder Operaciones**
A.7 Seguridad de los Recursos Humanos	**Coordinador RRHH**
A.8 Gestión de Activos	**Director Infraestructura TI + Líder Operaciones + Líder Comunicaciones**
A.9 Control de Acceso	**Director Infraestructura TI**
A.10 Criptografía	**Director Infraestructura TI + Líder Operaciones + director Soluciones**
A.11 Seguridad Física Y del Ambiente	**Director Infraestructura TI + Líder Comunicaciones**
A.12 Seguridad en las Operaciones	**Director Infraestructura TI + Líder Operaciones**
A.13 Seguridad de las comunicaciones	**Director Infraestructura TI + Líder Comunicaciones**
A.14 Adquisición, desarrollo y mantenimiento de sistemas de información	**Director Infraestructura TI + líder Soporte Técnico + director Soluciones**
A.15 Relación con Proveedores	**Director Infraestructura TI + director Tributaria y Legal**
A.16 Gestión de Incidentes de Seguridad de la Información	**Director Infraestructura TI**

A.17 Gestión de la Continuidad del Negocio	**Gerencia + Todos los Procesos**
A.18 Cumplimiento	**Director Infraestructura TI + Auditores + director Tributaria y Legal**

La Política General establece un marco global de los requisitos que se deben establecer para el desarrollo del PSI, ahora, realizaremos un recorrido tangencial por cada una de las políticas desarrolladas.

2 Políticas de Seguridad

Las políticas de seguridad definen el alcance que tendrá el PSI dentro de la organización y los controles necesarios a implementar para garantizar una gestión segura de la información.

2.1 Alcance

Teniendo en cuenta el contexto y la necesidad de la organización, el alcance PSI se define de acuerdo con los siguientes aspectos.

i. Procesos y áreas incluidas

El PSI aplica a todas las funciones, servicios, actividades y activos de información de Socia BPO.

Fig. 16. Mapa de procesos incluidos en el alcance PSI.

ii. Relación de servicios dentro y fuera del alcance

La relación entre los servicios internos de Socia BPO dentro del alcance del PSI y los que están fuera del alcance del PSI se identifican a continuación.

Los servicios que se encuentran fuera del alcance del PSI son aquellos en los que Socia BPO no tiene una injerencia técnica, por lo cual no puede garantizar un uso correcto en la seguridad de la información.

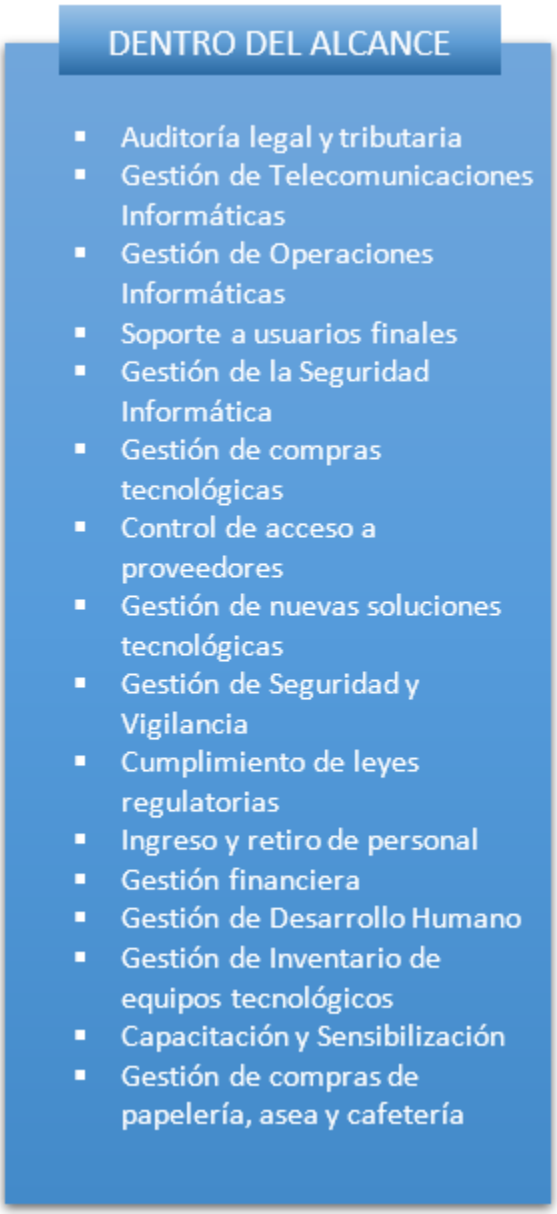

Fig. 17. Dentro del Alcance.

Fig. 18. Fuera del alcance.

Al prestar estos servicios Socia BPO confía en muchos proveedores externos que son contratados para proporcionar soluciones y servicios que pueden almacenar, procesar y generar información o que pueden tener acceso a la información de Socia BPO.

Socia BPO también está obligado a compartir información con instituciones del gobierno y otras instituciones externas debido a requisitos legales, regulatorios, o comerciales.

Socia BPO protege la confidencialidad, integridad y disponibilidad de información que se encuentra en ubicaciones de proveedores que están fuera del alcance del PSI al garantizar procesos de adquisición sólidos, contractuales y que existen acuerdos para compartir información.

iii. Unidades organizativas

La estructura organizacional de la Seguridad de la Información de Socia BPO corresponde al esquema definido y aprobado, en donde se identifican las dependencias funcionales y estratégicas de Socia BPO.

Socia BPO emplea una fuerza laboral de 40 personas para recopilar y procesar información, con el objetivo de permitir la prestación de los servicios anteriormente descritos.

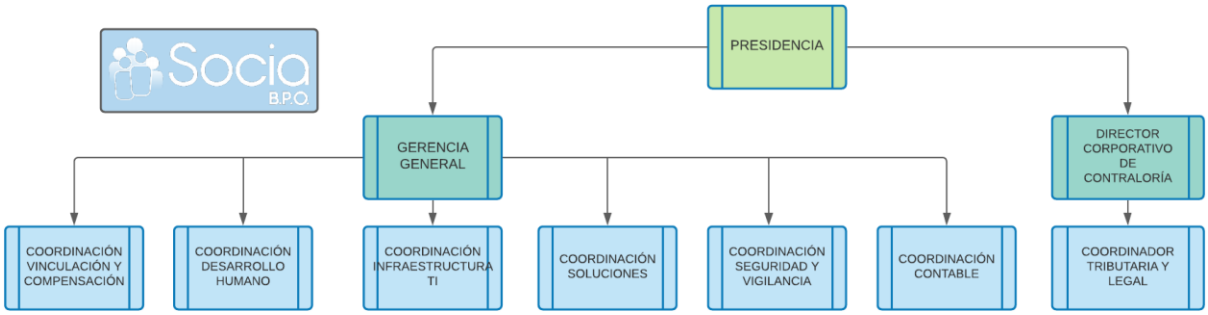

Fig. 19. Estructura organizacional de Socia BPO.

iv. Ubicaciones

La ubicación principal de Socia BPO se encuentra en la ciudad de Medellín, en la sede de Palacé en el segundo piso del edificio de Agenciauto.

Por regulaciones del gobierno nacional de Colombia los funcionarios de Socia BPO pueden ejercer el trabajo en casa.

v. Redes de datos

TABLA II
REDES DE DATOS

SEGMENTO RED CORPORATIVA	VLANS
10.4.2.0/23	2 - DATOS
10.4.5.0/24	3 – TELEFONÍA
172.16.1.0/24	4 – WIFI CLIENTES
10.4.0.0/24	5 – SERVICIOS LOCALES
10.4.6.0/27	6 – IMPRESORAS
192.168.150.0/24	7- SEGURIDAD
10.4.7.64/27	8 – CONTACT CENTER
10.4.7.240/28	12 – SRV_TELEFONÍA
10.254.10.0/24	10 – ADMIN SWITCHES
10.4.1.0/24	MZ SERVIDORES
172.27.164.64/27	MZ SERVIDORES WEB

vi. Servidores

Socia BPO comparte recursos de servidores con otras empresas, por esta razón, estos servidores deben entrar en el alcance de la implementación del Plan de Seguridad, pues es

necesario proteger la confidencialidad, integridad y disponibilidad de la información de Socia BPO sin importar dónde se encuentra ubicada física y lógicamente.

TABLA III
SERVIDORES

NOMBRE	USO
HEFESTO	PRODUCCIÓN
POSEIDON	PRODUCCIÓN
HEIMDALL	PRODUCCIÓN
ANUBIS	PRODUCCIÓN
HORUS	PRODUCCIÓN
TEBAS	PRODUCCIÓN
FRIGGA	PRODUCCIÓN
PBX_HOLDING	PRODUCCIÓN
SOKAR	PRODUCCIÓN
ATENEA	PRODUCCIÓN
ZAYA	PRODUCCIÓN
ISIS	PRODUCCIÓN
HATHOR	PRODUCCIÓN
ARTEMIS	PRUEBAS
HAPY	PRODUCCIÓN
CASSIOPEIA	PRODUCCIÓN
NEPTUNO	PRODUCCIÓN
DEMETER	PRODUCCIÓN
QAE	PRODUCCIÓN
CRONO	PRODUCCIÓN
HELIOS	PRUEBAS
WOLE	PRODUCCIÓN
HEBE	PRUEBAS
HERMES	PRODUCCIÓN
DIONISIO	PRODUCCIÓN

QAW	PRODUCCIÓN
EROS	PRODUCCIÓN - PRUEBAS
ARTEMISA	PRODUCCIÓN
HERACLES	PRODUCCIÓN
CRATOS	PRODUCCIÓN
KEPHIRI	PRODUCCIÓN
AFRODITA	PRODUCCIÓN
AURA	PRODUCCIÓN
CERES	PRODUCCIÓN
PAN	PRODUCCIÓN

2.2 Especificación de controles de Seguridad de la Información

Dominio	Control	Descripción del control	Riesgo Asociado	Código de Riesgo	Entregable
7. SEGURIDAD DE LOS RECURSOS HUMANOS	7.2.2. Educación y formación en la seguridad de la información	Realizar divulgación de la Política y normativa de seguridad de la información a los empleados, y/o terceros de proyectos que impliquen cambios sobre la infraestructura o aplicaciones productivas o nuevas.	Pérdida de integridad, confidencialidad y/o disponibilidad de la información por incumplimiento o desconocimiento de normativa	R1	Registro de las divulgaciones realizadas donde se evidencie: -Tema de la divulgación -Fecha de divulgación -Lista de asistencia
9. CONTROL DE ACCESO	9.2.2. Suministro de acceso de usuarios	Verificar que el nivel de acceso otorgado a los usuarios corresponde a las políticas de acceso, manteniendo un registro central	Perdida de Integridad, confidencialidad y/o disponibilidad de la información debido a actividades no autorizadas debido a: Acceso de personal no autorizado privilegios o permisos no adecuados. Falta de segregación de funciones.	R2	Matriz de usuarios con privilegios asociados y segregación de funciones aprobado. Documento de definición de los aprobadores de los accesos al sistema de información solicitados.
	9.2.3. Gestión de derechos de acceso privilegiado.	Se deberá tener un registro de todos los privilegios asignados			
	9.4.1. Restricción de acceso a la información.	Restringir el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones			
9. CONTROL DE ACCESO	9.2.2. Suministro de acceso de usuarios	Implementar un módulo de administración de usuarios y roles para acceder a sistemas de información y servicios que permita crear, modificar, eliminar, desactivar y/o bloquear usuarios y roles	Pérdida de integridad, confidencialidad y/o disponibilidad de la información por falta de administración centralizada de usuarios y los roles asociados. Daño a la imagen de la compañía por acceso a información no autorizada y divulgación de la misma.	R3	Evidencia de la existencia de un módulo de administración de usuarios donde se pueda crear, eliminar, modificar, desactivar y/o bloquear usuarios y roles
9. CONTROL DE ACCESO	9.2.3. Gestión de derechos de acceso privilegiado	Desactivar los usuarios genéricos o anónimos de los sistemas de información de carácter técnico. En el caso que se requieran se deberá soportar técnicamente su uso y se debe asignar formalmente a un responsable.	Actividades no autorizadas sobre la información debido a privilegios de un usuario no autorizado, generando pérdidas económicas, de imagen, pérdida de integridad, confidencialidad y disponibilidad de la información.	R4	* Registro de usuarios genéricos o anónimos de carácter técnico de los sistemas de información. * Documento técnico donde se justifique la creación y el uso de los usuarios genéricos y el responsable de su custodia, aprobad por el coordinador de Infraestructura TI
9. CONTROL DE ACCESO	9.4.2. Procedimiento de ingreso seguro 9.4.3. Sistema de gestión de contraseñas	*Tener un sistema de seguridad para la gestión de contraseñas donde se pueda: activar, modificar periódicamente, limitar histórico de contraseña, cifrar contraseña mientras se digita, tiempo de inactividad, etc *Mecanismos de trasferencia segura, tales como SSL, TLS y SSH.	Fuga de información, pérdida de confidencialidad de la información, accesos no autorizados debido a debilidades en seguridad de contraseñas	R5	Evidencia de los parámetros de configuración de seguridad para el uso de las contraseñas de acuerdo a la política de control de acceso.
12. SEGURIDAD DE LAS OPERACIONES	12.1. Procedimientos Operacionales y Responsabilidades	Documentar los procedimientos operativos y dejar a disposición de todos los usuarios que los necesiten.	Perdida de integridad, confidencialidad y/o disponibilidad de la información debido a la falta de gestión y conocimiento de la operación. Pérdidas económicas y de imagen de la empresa.	R6	Guía operativa de la solución donde se incluya lo siguiente: • Instalación y configuración • Manejo de la información (Digital, físico, etc.). • Actividades realizadas. • Manejo de errores y excepciones. • Niveles de escalamiento y comunicaciones. • Manejo de medios y elementos de salida. Manuales técnicos de Operación
	12.3.1. Copias de respaldo	Acordar y establecer el tipo de respaldo, la frecuencia y el tiempo de retención de los mismos.	Fallas y demoras en la operación de la solución debido a falta de establecimiento de políticas de backup ocasionando pérdida de disponibilidad de la información.	R7	* Registro de política de copia de respaldo definida y aprobada. * Evidencia de generación de copias de respaldo * Plan de pruebas de restauración que incluyan el procedimiento de restauración
	12.4.3. Registros del administrador y del operador 12.4.4. Sincronización de relojes	Acordar y definir los registros de auditoría para los eventos que se consideren como críticos de los componentes de infraestructura que soportan el sistema de información. La infraestructura deberá contar con sincronización de relojes ajustada.	* Pérdida de confidencialidad, integridad y disponibilidad de la información por actividades no autorizadas debido a falta de configuración de eventos o logs de auditoria no definidos adecuadamente * Perdidas económicas y de imagen de la empresa	R8	* Registro de eventos críticos definidos.. * Evidencia de captura de generación de eventos. * Evidencia de sincronización de relojes de la infraestructura
	12.4. Gestión de la Vulnerabilidad Técnica	Gestionar y remediar las vulnerabilidades críticas, altas y medias generadas en cada infraestructura y sistema de información	Pérdida de integridad, confidencialidad y disponibilidad de la información por exploración de vulnerabilidades Perdidas económicas y de imagen de la empresa	R9	* Evidencia de reporte de vulnerabilidades con 0 criticas, altas y medias. * En caso que no sea posible cerrar alguna vulnerabilidad, soporte técnico justificado del no cierre de la misma con aprobación.
13. SEGURIDAD DE LAS COMUNICACIONES	13.1. Gestión de la seguridad en las redes	Definir e Identificar las medidas de seguridad implementadas en la solución	pérdida de disponibilidad y confidencialidad de la información por falta de aseguramiento de las redes	R10	* Diagrama de red detallado de la solución implementada donde se incluyan soluciones de seguridad tales como firewalls, SDWAN, MPLS, WAF etc. Tambien debe incluir direccionamiento y puertos habilitados.
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	14.1. Requisitos de Seguridad de los Sistemas de Información 12.1.1. Documentación de procedimientos de operación 14.2.9. Pruebas de aceptación	Verificar que las pruebas de seguridad realizadas cumplen con lo requerido incluyendo la aplicabilidad de las listas de endurecimiento (hardening) para la infraestructura de la solución	Fallas en la operación de la infraestructura que soportan las soluciones debido a no cumplimiento de aplicabilidad de lineamientos definidos por seguridad lo que conlleva a falta de disponibilidad, integridad y confidencialidad de la información.	R11	*Acta de cumplimiento de requisitos de seguridad. *Registro de cumplimiento de las guías de aseguramiento
15. RELACIONES CON LOS PROVEEDORES	15.1.1. Política de seguridad de la información para las relaciones con proveedores 15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores	Adjuntar a los contratos con proveedores la política de seguridad de la información	Pérdida o fuga de información debido a falta de especificación de cumplimientos de seguridad contractuales con proveedores para adquisición o mantenimiento de soluciones. Pérdidad económicas y multas por incumplimientos legales	R12	* Contrato con proveedor donde se evidencie adjunta la política de seguridad de la información para proveedores, acuerdo de privacidad y derechos de autor * Acuerdo de confidencialidad firmado por el personal.
18. CUMPLIMIENTO	18.1.4 Privacidad y protección de información de datos personales. 15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores 13.2.4. Acuerdos de confidencialidad	Incluir cláusulas de confidencialidad, derechos de autor o licenciamiento,política de datos personal si aplica en los contratos de adquisición o modificación de soluciones, según aplique			
17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO	17.1.1 Planificación de la continuidad de la seguridad de la información	Definir y documentar el plan de continuidad para la solución tecnológica del sistema de información.	Pérdida de disponbilidad e integridad del servicio debido a interrupciones inesperadas por falta de un plan de continuidad	R13	* Documento DRP (Plan de Recuperación de Desastres) para la solución tecnológica.
17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO	17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Realizar prueba de continuidad para la solución tecnológica del sistema de información		R14	*Plan de pruebas de continuidad de la solución

Fig. 20. Control de requisitos.

3 Organización de la información

La organización de la información se abordó en dos controles específicos, los cuales fueron incluir en el contrato laboral una cláusula de seguridad de la información que garantice que los empleados que acceden a la información van a cumplir los requisitos de seguridad establecidos por la organización, así mismo, se realizó un acuerdo de confidencialidad para aquellos proveedores, contratistas o externos que requieran acceder a la información confidencial de la organización, estos documentos fueron validados y aprobados por el abogado de la organización con el fin de garantizar que se encuentra dentro del marco legal.

4 RRHH

El área de gestión humana realiza las investigaciones necesarias para garantizar que los empleados que se contratan en la organización cumplen con todos los requisitos legales, esto incluye verificación de antecedentes, referencias personales y laborales y se realiza visita domiciliaria, una vez que el empleado cumple con todos los requisitos, gestión humana se encarga de realizar las solicitudes al área de TI para dar de alta al usuarios y asignar los accesos y recursos necesarios para que pueda desempeñar sus funciones, adicional, se encarga de realizar la inducción la cuál incluye los deberes que tiene con el cumplimiento de los requisitos de seguridad de la información.

5 Gestión de Activos

La gestión de activos enmarca las políticas de Uso Adecuado de Activos y la Gestión de Activos, así mismo, establece las estrategias para el tratamiento del riesgo y la clasificación de la información.

5.1 Uso Adecuado de Activos

El uso adecuado de activos establece los parámetros que deben cumplir los empleados de la organización con los recursos asignados y disponibles para llevar a cabo sus funciones, además, esta define que la organización podrá monitorear, revisar y reportar en cualquier momentos las

actividades realizadas por los colaboradores con el fin de garantizar el correcto uso de los activos informáticos de la compañía, también, establece que toda la información enviada y recibida, contenida y procesada o generada con activos tecnológicos de la organización son propiedad de esta.

La política de Uso Adecuado de Activos cubre el uso del Internet, correo electrónico y mensajería instantánea dentro de la organización, las responsabilidades de los colaboradores con el uso de contraseñas y servicios que se disponen para llevar a cabo sus funciones, así mismo, se establece la responsabilidad de estos con los equipos de cómputo y dispositivos móviles, esto establece los lineamientos para trabajar en las redes corporativas y cómo puede solicitar servicio de soporte técnico, ya que está prohibida la manipulación de los equipos por parte de los empleados; esta política también define las normas establecidas con respecto a la seguridad en el puesto de trabajo, se refiere específicamente a no dejar el equipo desbloqueado en su ausencia, ni documentos confidenciales en su puesto de trabajo, finalmente, se define la política de daños a cargo del colaborador donde la empresa podría cobrar este en caso de comprobarse dolo o culpabilidad en el daño de este.

Esta política es difundida en las inducciones y reinducciones de la organización y se encuentra publicada en la intranet para que pueda ser consultada en cualquier momento por los empleados.

5.2 Gestión de Activos

Esta política define los lineamientos para las responsabilidades de los activos, el inventario, la propiedad de los activos, la devolución de activos, clasificación de la información y el etiquetado.

i. Responsabilidad de los Activos

- Cada empleado de la compañía es responsable por el buen uso y gestión de los activos fijos que estén a su cargo.
- Cada activo asignado será entregado con su acta FTIN013 - ACTA DE ENTREGA DISPOSITIVO la cual debe ser firmada por quien recibe y quien hace la entrega por parte del área de Tecnología Informática.

- Cuando los activos se encuentren en custodia del área de Tecnología Informática este será responsable por el buen cuidado mientras se reasigne, reubique o deseche.

ii. Inventario de Activos

- Todos los recursos tecnológicos que administra el área de Tecnología Informática deben ser registrados y controlados desde la plataforma de Gestión de Soporte Técnico.
- Cada activo tecnológico debe estar asignado a un responsable dentro de la organización y relacionado con el inventario que se encuentra en la plataforma de Gestión de Soporte Técnico.

iii. Devolución de Activos

- En el momento que un usuario termina la relación laboral con la compañía se debe validar los activos tecnológicos que tiene asignado actualmente en el inventario, se deberá reportar al área de Vinculación y Compensación por medio de correo electrónico y/o por medio del documento de Paz y Salvo.
- El Paz y Salvo solo podrá ser firmado por el líder de Soporte Técnico previa validación del estado de los activos. De no estar en conformidad se debe reportar al área de Vinculación y Compensación.
- Los activos tecnológicos deberán ser recogidos y/o recibos 1 día hábil después de la terminación de la relación laboral. El área de Compensación debe exigir esta paz y salvo para liquidar al usuario.
- Una vez que sea recibido el equipo, se deberá realizar un mantenimiento físico y lógico. Se elimina el perfil del usuario anterior y se crea uno nuevo. Si el equipo de cómputo cambia de área es obligatorio realizar el formateo de la máquina.
- Se realizará un borrado a bajo nivel solamente a los equipos de cómputo que fueron usados por las áreas administrativas de la empresa.

iv. Clasificación de la Información

- Se clasifica la información/activos con base en el procedimiento establecido en el PRIN022 – CLASIFICACIÓN DE ACTIVOS

- Se deberá tener en cuenta la información que está regulada por la Ley 1581 de 2012 [Protección de datos personales] y ley 1266 de 2008 [hábeas data] para darle la clasificación y el tratamiento requerido por esta.
- El dueño de la información es el responsable por clasificar la información de acuerdo con su criticidad y con base en el procedimiento PRIN022 – CLASIFICACIÓN DE ACTIVOS.
- La clasificación de la información debe ser exactamente igual para toda la organización.
- El nivel de protección que se le dará a la información estará dado por los criterios de disponibilidad, confidencialidad e integridad definidos en PRIN022 – CLASIFICACIÓN DE ACTIVOS.

TABLA IV
CRITERIOS DE CLASIFICACIÓN DE LA INFORMACIÓN

Clasificación	Descripción
Confidencial	Es un activo crítico y tiene un nivel de confidencialidad mayor.
Restringida	Tienen un nivel de confidencialidad medio.
Interno	Información con nivel bajo de confidencialidad, su uso está limitado a los funcionarios de la organización
Público	Cualquier persona puede ver la información.

v. Etiquetado de Activos de Información

Los activos de la organización se identifican y se registran cuando tienen un valor económico considerable, a continuación, se definen los activos que se identificarán y se registran y los que no se les realizará este proceso, también se define el estándar de etiquetado de cada uno.

- Los servidores se identifican con base en nombres de dioses griegos.
- El estándar de identificación se define por las iniciales de la empresa siguiente del consecutivo del activo, por ejemplo, SC0005, no se diferencia tipo de Activo.

TABLA V
ETIQUETACIÓN ACTIVOS

Incluidos en la etiquetación	Excluidos de la etiquetación
Portátiles	Teclado
ALL in ONE	Mouse
Workstation	Bases refrigerantes
Teléfonos	Guayas de Seguridad
Cámaras de videoconferencias	Maletines
Televisores	Adaptadores
Impresoras	Cables de Red y video
Servidores	Herramientas
Switches	Diademas
Antenas Wifi	Celulares
UPS	
QNAPS	
Monitores	
Proyectores	
Arañas de Telecomunicación	
Tabletas	
Raspberry	
ATA	
Cámaras fotográficas	
Scanner	
MiFi	

5.3 Procedimiento para la Clasificación de Activos

En el proceso de seguridad de la información es indispensable contar con la metodología para clasificación los activos dependiendo de su criticidad, por ello, a continuación, se define una tabla de valoración de activos que depende de tres dimensiones de gran importancia para garantizar una correcta implementación del Plan de Seguridad de la Información, las cuales son: Confidencialidad, Integridad y Disponibilidad.

i. Confidencialidad

La confidencialidad se refiere a que la información debe llegar únicamente a las personas autorizadas. Esta es definida según las características de la información gestionada y procesada por el activo. Para la presente valoración se toman en cuenta los siguientes criterios de clasificación.

TABLA VI
CRITERIO CLASIFICACIÓN ACTIVOS – CONFIDENCIALIDAD.

Escala de valoración	Valor	Confidencialidad	
3	Alto	El activo gestiona y/o procesa información reservada, su uso inadecuado puede generar consecuencias graves para la organización.	Información disponible sólo para un proceso de la organización y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.
2	Medio	El activo gestiona y/o procesa información clasificada, su uso inadecuado puede generar medianas consecuencias a la organización, como, por ejemplo, reclamaciones de las áreas que soporta.	Información disponible para todos los procesos de la organización y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de esta. Esta información es propia de la organización o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.

1	Bajo	El activo gestiona y/o procesa información pública, no genera consecuencias negativas para la organización.	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la organización, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.
0	No clasificada	Activos de información que deben ser incluidos en el inventario y que aún no han sido clasificados.	Deben ser tratados como activos de INFORMACIÓN RESERVADA hasta el momento en que se defina una valoración entre la escala del 1-3 definida.

ii. Integridad

La integridad es una característica o propiedad de la información que garantiza que esta no ha sido alterada (modificada o destruida) de manera no autorizada.

Los criterios de valoración de integridad para los activos de Socia BPO se describen a continuación

TABLA VII
CRITERIO CLASIFICACIÓN ACTIVOS – INTEGRIDAD.

Escala de Valoración	Valoración	Integridad
3	Alto	El activo gestiona Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la organización. Es información que apoya la toma de decisiones estratégicas de la organización. Los errores deben ser solucionados de inmediato.
2		El activo gestiona Información cuya pérdida de exactitud y completitud puede conllevar un impacto

	Medio	negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderada a funcionarios de la organización. La información gestionada por el activo permite una brecha de errores que pueden ser solucionados a corto plazo.
1	Bajo	El activo gestiona Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la organización o entes externos. Los errores pueden ser solucionados en un mediano plazo
0	No clasificada	El activo de información debe ser incluido en el inventario y aún no ha sido clasificado. Debe ser tratado como activo de Integridad nivel 3 hasta el momento en que se defina una valoración entre la escala del 1-3 definida.

iii. Disponibilidad

La disponibilidad asegura que los usuarios autorizados tienen acceso a la información y activos asociados cuando lo requieren, es decir, con esta propiedad se previene la denegación de acceso a datos y servicios de información autorizados. En la tabla se presentan los criterios de valoración de disponibilidad para los activos de la organización.

TABLA VIII
CRITERIO CLASIFICACIÓN ACTIVOS – DISPONIBILIDAD.

Escala de Valoración	Valoración	Disponibilidad
3	Alto	El activo apoya los procesos críticos de la organización y se requiere de una recuperación inmediata en caso de falla. Puesto que, la no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.

2	Medio	El activo apoya los procesos no críticos de la organización y permite su recuperación en un tiempo no mayor a 3 días. Puede generar repercusiones económicas, legales o de imagen moderadas.
1	Bajo	El activo apoya los procesos no críticos de la organización y permite su recuperación en un tiempo superior a 3 días. La no disponibilidad de la información puede afectar la operación normal de la organización o entes externos, pero no conlleva implicaciones legales, económicas o de imagen.
0	No clasificada	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados. Deben ser tratados como activos de Disponibilidad de nivel 3 hasta el momento en que se defina una valoración entre la escala del 1-3 definida.

5.4 Valoración del Riesgo

La valoración del riesgo permite estimar la magnitud de los riesgos a los que está expuesta la organización. La materialización de una amenaza consta de dos elementos: probabilidad e impacto, estos determinan el nivel del riesgo.

De acuerdo con la probabilidad se determinan los siguientes criterios de valoración:

TABLA IX
VALORACIÓN DEL RIESGO.

Escala de valoración	**Valoración**	**Descripción**
3	Alto	La amenaza se puede materializar mínimo una vez al mes
2	Medio	La amenaza se puede materializar a lo sumo una vez en el semestre
1	Bajo	La amenaza se puede materializar a lo sumo una vez al año

Según el impacto se determinan los siguientes criterios de evaluación:

TABLA X
IMPACTO DEL RIESGO.

Escala de valoración	Valoración	Descripción
3	Alto	La ocurrencia del evento tiene impacto a nivel de confidencialidad, integridad y/o disponibilidad de la información poniendo en riesgo la reputación de la empresa y/o inconvenientes legales.
2	Medio	La ocurrencia del evento tiene impacto a nivel de confidencialidad, integridad y/o disponibilidad de la información sin poner en riesgo la reputación de la empresa o necesidad de medidas legales.
1	Bajo	La ocurrencia del evento no tiene consecuencias relevantes para la organización.

Por la combinación probabilidad – impacto se define el mapa de riesgo que se presenta a continuación, los números en el interior de las celdas son calculados por la multiplicación de la probabilidad x impacto. Se indican por medio de los tonos de colores la criticidad del riesgo.

TABLA XI
MAPA DEL RIESGO.

MAPA DE RIESGO				
Probabilidad	3 - Alta	3	6	9
	2 - Media	2	4	6
	1- Baja	1	2	3
		1 - Bajo	2 - Medio	3 -Alto
	Impacto			

5.5 Plan de tratamiento del Riesgo

La principal estrategia para el tratamiento de riesgo es estudiar la situación y determinar en cuáles de los siguientes casos se ubica el riesgo, con el propósito de enfocarse en el objetivo correcto.

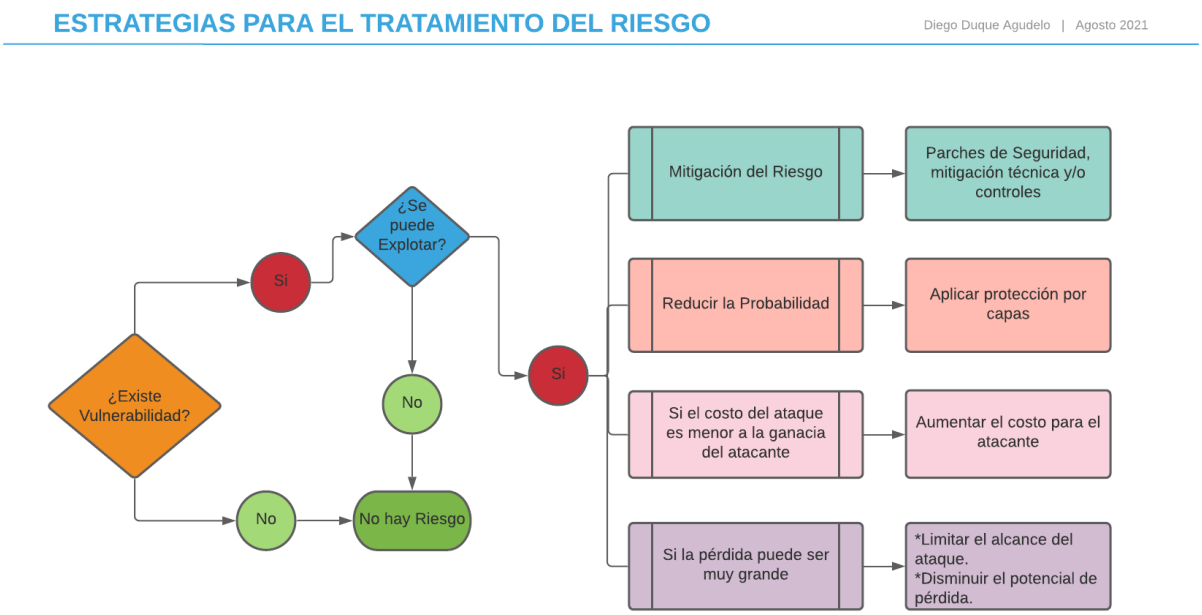

Fig. 21. Estrategias para el tratamiento del riesgo.

- Cuando existe una vulnerabilidad (defecto, debilidad) es necesario implementar técnicas que garanticen la reducción de la probabilidad de que la vulnerabilidad sea explotada.
- Cuando se puede explotar una vulnerabilidad es necesario aplicar protección en capas, diseños arquitectónicos y controles administrativos para minimizar el riesgo o prevenir esta ocurrencia.
- Cuando el costo del ataque es menor que la ganancia potencial para el atacante es necesario aplicar protección para disminuir la motivación aumentando el costo del atacante (por ejemplo, usar controles del sistema para limitar lo que un usuario puede hacer).
- Cuando la pérdida puede ser demasiado grande, es necesario aplicar principios de diseño, técnicas y procedimientos para limitar el alcance del ataque, reduciendo así el potencial de pérdida.

A partir de lo anterior se definen las siguientes estrategias:

TABLA XII
ESTRATEGIAS DEL TRATAMIENTO DEL RIESGO.

ESTRATEGIAS PARA TRATAMIENTO DE RIESGO				
Probabilidad	3 - Alta	3.Zona de riesgo Moderado Tratamiento: Reducir la probabilidad de ocurrencia Evitar el riesgo	6. Zona de riesgo extremo Tratamiento: Reducir el riesgo Evitar el riesgo Compartir o transferir	9.Zona de riesgo Extremo Tratamiento: Reducir el riesgo Evitar el riesgo Compartir o transferir
	2 - Media	2. Zona de riesgo Bajo Tratamiento: Reducir la probabilidad de ocurrencia	4.Zona de riesgo Moderado Tratamiento: Reducir el riesgo Evitar el riesgo	6. Zona de riesgo extremo Tratamiento: Reducir el riesgo Evitar el riesgo Compartir o transferir
	1 - Bajo	1. Zona de riesgo Bajo Tratamiento: Asumir el riesgo	2. Zona de riesgo Bajo Tratamiento: Reducir el riesgo Evitar el riesgo	3.Zona de riesgo Moderado Tratamiento: Reducir el riesgo Evitar el riesgo
		1 - Bajo	2 - Medio	3 - Alto
	Impacto			

De acuerdo con el nivel de riesgo detectado estos se pueden aceptar, evitar, controlar, investigar, mitigar o transferir.

6 Control de Acceso

El Plan de Información de Seguridad controla el acceso a la información y a los medios de procesamiento a esta, propendiendo por mantener los criterios de seguridad y calidad.

Como buena práctica y en camino a proteger la información se define como política general de control de acceso que todo está prohibido a menos que esté expresamente permitido.

6.1 Autenticación de usuarios para conexiones externas

- La autenticación de los usuarios remotos se realizará únicamente por la Red Privada Virtual (VPN) de la empresa, debe usar el usuario y la clave asignada para tal fin.
- El acceso remoto a información reservada y/o confidencial se establecerá bajo esquemas que provean cifrado (conexiones VPN SSL). Es importante mencionar que el acceso se realizará de acuerdo con los perfiles establecidos en el Directorio Activo y las políticas específicas configuradas en el Firewall.
- No se permite la utilización de cuentas (root, admin, user […]) o contraseñas genéricas.
- La dificultad de las contraseñas será la definida en la política PLIN018 – GESTIÓN DE CONTRASEÑAS
- Las autenticaciones de usuarios para conexiones externas serán registradas en los logs de auditoría.

6.2 Acceso de los equipos a las redes corporativas

El área de Tecnología Informática aplicará el principio de menor privilegio posible para la conexión de un usuario a la red, de esta forma la conexión desde y hacia redes compartidas debe ser restringida a quienes requieren el acceso y solo con privilegios requeridos.

No se permite el acceso a la red corporativa en equipos personales a menos que cumplan con los controles de seguridad establecidos, en este caso debe ser autorizado por el personal del área de Tecnología Informática. Los equipos deben cumplir con los siguientes requisitos:

- Sistema Operativo licenciado y con los parches aplicados
- Office actualizado y licenciado
- Antivirus licenciado y actualizado

El acceso a equipos especializados de cómputo (servidores, enrutadores, bases de datos, servidores centralizados, switches [...]) conectado a la red debe ser administrado por el personal autorizado por el director de Tecnología Informática.

En el momento de modificar la contraseña de acceso a los diferentes componentes de red, debe cumplir con lo establecido en la PLIN018 – POLÍTICA DE GESTIÓN DE CONTRASEÑAS se debe tener en cuenta que esto depende del tipo de dispositivo/aplicación/servidor al que se le vaya a aplicar el cambio de contraseña.

6.3 Protección de los puertos de configuración y diagnóstico remoto

- El acceso físico y lógico a los puertos de configuración de la infraestructura tecnológica están restringidos y controlados exclusivamente para los responsables de dichas actividades.
- Los puertos físicos y lógicos que no se usen, deben ser desactivados/inhabilitados.
- La solicitud de apertura de un puerto lógico TCP/UDP se debe realizar por escrito al director del área de Tecnología Informática.
- Se debe tener un inventario actualizado de los puertos expuestos a Internet y su uso.

6.4 Controles de Acceso

Se ha establecido una metodología para la definición de roles y perfiles para los colaboradores y terceros de acuerdo con la función a desempeñar, de tal forma que la información sólo sea accesible por los usuarios autorizados, y con base en la clasificación de la información.

Se realiza un control periódico de las cuentas de usuario, con el propósito de mantener activas sólo las que deban permanecer vigentes.

6.5 Gestión de privilegios

- No se otorgan privilegios hasta que se complete el proceso de autorización.
- Cada sistema de información y/o plataforma gestionada estará a cargo de un especialista, quien se encargará de las modificaciones a los privilegios o perfiles de usuario.
- Los privilegios especiales del sistema se otorgarán únicamente a los especialistas. Los usuarios finales de los sistemas de información no deben tener acceso a los niveles de administración para el funcionamiento del sistema.

- El protocolo PTIN008 - PERFILES DE USUARIOS debe mantenerse actualizado y los permisos privilegiados deben gestionarse con base en esta.
- Los usuarios de acceso privilegiado deben usar factores de doble autenticación mientras sea posible.

6.6 Revisión de los derechos de Acceso

Una vez por año el líder de seguridad de la información valida los permisos de acceso a las aplicaciones y/o servicios de los empleados y/o terceros. Dentro de las validaciones de seguridad a realizar están:

- Verificar que los usuarios activos en el dominio y en los sistemas de información tengan los permisos de acuerdo con su perfil y funciones, y de ser necesario realizar los ajustes pertinentes.
- Validar que no existan cuentas de usuario activas y asignadas a excolaboradores o personal externo que no esté laborando.
- Periódicamente el director y líder efectuará una revisión a los permisos de los usuarios de la infraestructura tecnológica.
- Se genera un informe con los resultados de la revisión de usuarios y de permisos.

6.7 Control de Acceso a los sistemas y aplicaciones

- Después de cinco intentos consecutivos fallidos de ingreso al sistema de información, se bloqueará el acceso de la cuenta de usuario, después de 15 minutos se desbloqueará nuevamente.
- Las palabras clave tendrán una longitud mínima de 10 caracteres, de los cuales al menos dos caracteres deben ser alfabético en minúscula, dos en mayúscula, un carácter no alfabético y dos numéricos.
- Las contraseñas no se presentarán en texto claro por ningún medio.
- El sistema obligará automáticamente a que las contraseñas de las cuentas de usuarios se cambien al menos una vez cada (42) días.
- El sistema controlará el tiempo de inactividad del usuario y bloqueará la sesión automáticamente después de 10 minutos.
- Los usuarios deben cumplir con la política de contraseñas establecida.

7 Criptografía

Se utilizan controles criptográficos en los siguientes casos:

- Para la protección de claves de acceso a sistemas, datos y servicios.
- Para la transmisión de información clasificada y/o reservada.
- Para proteger la información almacenada en los equipos de cómputo portátiles mediante BitLocker.
- Para el envío de archivo del pago de la nómina de empleados y pago a proveedores.

El área de Infraestructura Tecnología Informática debe verificar que todo sistema de información o aplicativo que requiere realizar transmisión de información reservada o confidencial, cuente con mecanismos de cifrado de datos.

- El acceso a aplicaciones de gestión y/o consolas de dispositivos de seguridad deben hacer uso de certificados digitales.
- Las páginas web, aplicaciones, API y cualquier servicio web debe contar con su certificado de seguridad.
- La información clasificada como reservada, debe almacenarse en un repositorio seguro (SharePoint), garantizando así la confidencialidad.
- Los medios removibles que contengan información reservada, y que deban salir de las instalaciones, deberán hacer uso de esquemas de cifrado.
- La renovación de los certificados se realizará cada año en el caso que sean comerciales, cuando el servicio sea ofrecido por Let’s Encrypt se realizará cada tres meses.
- Mientras sea posible se usarán métodos criptográficos gratuitos.
- Se emplea la criptografía para ofrecer los siguientes servicios de seguridad:
    - Servicios de confidencialidad.

7.1 Gestión de Claves

- Las claves criptográficas deben estar disponibles operativamente, tanto tiempo como lo requiera el servicio criptográfico correspondiente.
- Las llaves de BitLocker serán guardadas y gestionadas desde el Directorio Activo y Azure Directory.
- Las llaves de los certificados de seguridad deben ser guardadas en forma segura en la plataforma de gestión de contraseñas Keeper, garantizando que solo tendrán acceso los gestores de los certificados.

8 Seguridad Física y del Ambiente

8.1 Áreas seguras.

i. Perímetro de seguridad

Los perímetros de seguridad contarán con protección tales como paredes, puertas de entrada controladas por acceso biométricos y/o llaves, CCTV, alarmas y vigilancia física con el fin de proteger las áreas que contienen información y medios de procesamiento de información.

ii. Área Restringida

Se consideran áreas restringidas los siguientes:

- Centros de datos
- Cuarto de archivado
- Centro de vigilancia por CCTV
- Oficinas de directivos de la organización
- Oficina de Tecnología
- Oficina de Soluciones

iii. Controles de Acceso Físico y CCTV

Los siguientes lineamientos deben ser cumplidos para garantizar el control de acceso a las dependencias de la Organización:

- Las puertas de acceso a los centros de datos, áreas administrativas o almacenamiento de información confidencial o reservada deben permanecer

cerradas en todo momento, y el ingreso a las mismas debe estar limitado sólo al personal autorizado.

- Se debe documentar qué personal será autorizado para ingresar a las áreas restringidas, este debe permanecer actualizado en el tiempo.
- Cuando se de acceso a los proveedores a áreas restringidas como los centros de datos estos deberán cumplir con la política PLIN007 – ACCESO PROVEEDORES y cumplir con la documentación solicitada en el procedimiento PRIN001 – GESTIÓN DE INGRESO PROVEEDORES.
- La política de acceso al Circuito Cerrado de Televisión (CCTV) será definido en el documento PLIN004 – CONTROL DE ACCESO A CCTV.

iv. Seguridad de Oficinas, despachos e instalaciones

- Los proveedores deben permanecer con un distintivo de identificación como proveedor visible mientras se encuentren en las instalaciones de la organización.
- El ingreso en horario no laboral se debe tramitar por medio del Coordinador de Seguridad y Vigilancia previa solicitud del responsable de la actividad enviando por correo electrónico la solicitud de ingreso.

v. Protección contra amenazas externas y ambientales

- Mantener las condiciones físicas y ambientales óptimas para la protección de los centros de datos, así como controles automáticos para prevenir amenazas de incendios, inundaciones, aumentos de temperatura o humedad.
- Proporcionar el ambiente adecuado para conservación de medios de almacenamiento y equipos.
- Registrar en video las actividades en áreas públicas dentro de los confines de este tales como las puertas de acceso a zonas restringidas y las áreas de manipulación de información reservada y/o confidencial, mediante el uso de un circuito cerrado de televisión (CCTV), con el fin de mantener un control de seguridad.
- Mantener en condiciones óptimas de limpieza, seguridad, mantenimiento y funcionalidad cada uno de los elementos que forman parte del centro de datos.

- Los cuartos de datos deben contar con extintores que se ubiquen en la entrada de este, se debe realizar el control anual de vencimiento y funcionalidad.

vi. Trabajo en áreas seguras

- Solo se permite personal en las áreas restringidas cuando sea necesario realizar tareas específicas allí, previa autorización.
- Se debe supervisar las actividades realizadas por parte de los proveedores en las áreas restringidas.
- Mantener por un período de 1 año el registro de acceso del personal autorizado y de ingresos, con el objeto de facilitar procesos de seguimiento.
- Todos los sistemas de control de acceso deben ser monitoreados permanentemente.

8.2 Seguridad en los equipos

i. Ubicación y protección de los equipos

- Los centros de datos deben encontrarse localizados en el área restringida que cuente con medidas para prevenir inundaciones, robos, interferencias electromagnéticas, fuego, humo y demás amenazas que puedan interferir con su correcto funcionamiento y la continuidad del servicio que presta.
- Cuando el equipo deba estar ubicado en área comercial y/o recepción este deberá estar debidamente protegido por guaya de seguridad.
- Los centros de datos deben estar protegidos por acceso biométrico.
- Tanto los equipos ubicados en los centros de datos como los equipos de cómputo en las sedes deben estar conectados a la energía regulada.
- Los centros de datos deberán contar con aire acondicionado, de igual manera, este lugar debe permanecer cerrado para garantizar una baja temperatura, además, esto evitará que ingrese polvo adicional a los equipos.
- Se prohíbe comer, fumar y beber cerca de los equipos de cómputo, cualquier daño a estos por estas causas, se cobrará al responsable.
- Los equipos en los centros de datos NO se deben tocar si no es necesario su manipulación.

- Los equipos de los centros de datos SÓLO podrán ser manipulados por personal autorizado.

ii. Servicios de Suministro

- Se deben proteger los equipos contra fallas de energía y otras interrupciones originadas por ausencia de los servicios de soporte.
- Todos los servicios públicos de soporte, como electricidad, suministro de agua, desagüe, calefacción/ventilación y aire acondicionado, deben ser adecuados para los sistemas que soportan. Los servicios públicos de soporte deben ser inspeccionados regularmente y probados para asegurar su adecuado funcionamiento y para reducir cualquier riesgo de falla. Se debe proveer el suministro eléctrico de acuerdo con las especificaciones del fabricante del equipo.
- Se cuenta con dispositivos de suministro de energía ininterrumpida (UPS) para apoyar el funcionamiento continuo de los equipos que soportan las operaciones críticas del negocio.

iii. Seguridad del cableado

El cableado de la energía y el de las telecomunicaciones se protege contra la interceptación o daño.

Se consideran los siguientes lineamientos para el cableado:

- El cableado eléctrico y el cableado de datos (UTP) deben estar separados físicamente, así mismo, deben ir por ductería hasta su punta central, esto con el fin de evitar daño físico del mismo o interceptación de la información.
- Se debe evitar dentro de lo posible usar rutas públicas para la distribución del cableado
- Se utilizan estándares para la identificación y etiquetado de cables y equipos con el fin de minimizar errores en la manipulación, como una conexión a un punto de red incorrecto.
- Se debe mantener la documentación actualizada de las conexiones de red.

iv. Mantenimiento de los Equipos

Los equipos deben recibir un mantenimiento adecuado de acuerdo con el cronograma realizado para el año en curso.

- El área de Infraestructura Tecnología Informática realizará mantenimientos lógicos y físicos a los equipos de forma anual, dejando evidencias del proceso realizado.
- Los mantenimientos de los equipos de los proveedores de la infraestructura tecnológica serán requeridos por los propietarios de los equipos y de acuerdo con los lineamientos contractuales que se establezcan con cada proveedor.

Se deben considerar los siguientes lineamientos para el mantenimiento de los equipos:

- Sólo el personal autorizado puede llevar a cabo las reparaciones y el mantenimiento de los equipos.
- Se deben mantener registros de todas las fallas y todo mantenimiento preventivo y correctivo.

v. Retiro de activos

- Todo retiro de elementos, equipos o materiales fuera de la sede debe hacerse diligenciando el formato de salida y solicitando autorización por el jefe inmediato.
- El jefe inmediato podrá solicitar en cualquier momento el reintegro del activo al puesto de trabajo.
- El área de infraestructura podrá solicitar acercar el equipo en cualquier momento para efectos de mantenimiento.

vi. Seguridad de los equipos fuera de las instalaciones

- Los equipos fuera de la instalación deben estar debidamente inventariados y con un responsable asignado.
- Los equipos de cómputo deben tener la unidad de almacenamiento cifrado con BitLocker como se define en la política PLIN013 – CONTROLES CRIPTOGRÁFICOS

- Los equipos deben estar protegidos por contraseña de acceso.
- Los celulares deben estar protegidos por contraseña, pin, acceso biométrico […]
- Los celulares deberán tener la opción de borrado remoto activo.

vii. Seguridad en la reutilización o eliminación de los equipos

- Cuando un equipo se necesite reutilizar, trasladar o dar de baja, se debe eliminar toda información residente en los dispositivos de almacenamiento, utilizando el procedimiento PRIN024 – BORRADO DE INFORMACIÓN.
- En caso de dar de baja el equipo, se debe realizar la destrucción física del medio de almacenamiento, utilizando impacto, fuerzas o desarme completo y realizar la disposición adecuada de este tal como se nombra en la política PLIN006 – GESTIÓN DE ACTIVOS DE INFORMACIÓN.

8.3 Procedimiento ingreso visitantes y proveedores

El procedimiento descrito en la Fig. 22 hace referencia el flujo que se debe llevar a cabo para que un visitante, proveedor o contratistas ingresar a las instalaciones de la organización.

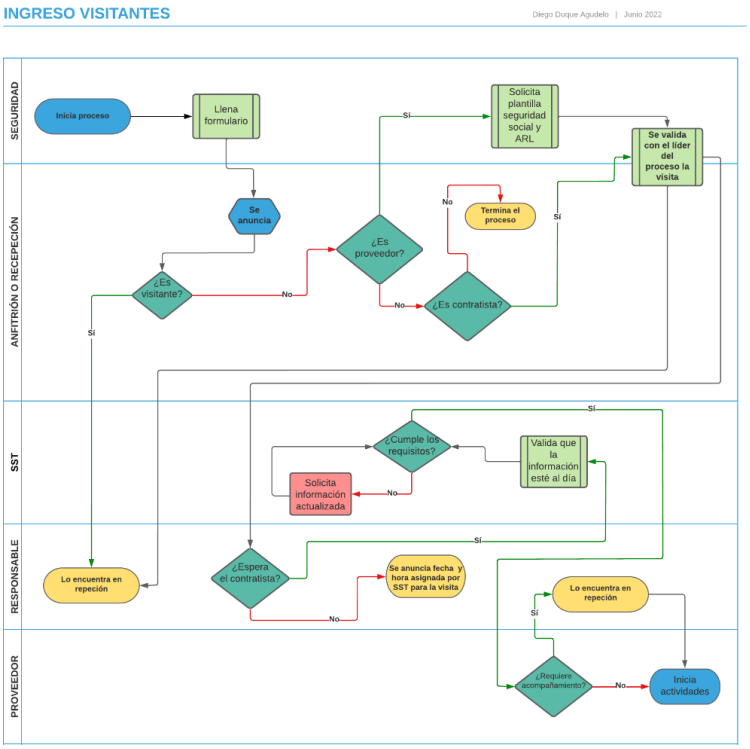

Fig. 22. Ingreso de visitantes.

9 Seguridad de las Operaciones y Comunicaciones

La Seguridad de las Operaciones y las Comunicaciones contienen información confidencial para la organización, por lo que nombraré de forma general las políticas desarrolladas para estos dominios.

9.1 Seguridad Operaciones

Las políticas generadas para salvaguardar la seguridad de las operaciones son las siguientes:

- **Responsabilidades y procedimientos de operación:** Las cuales tienen como función garantizar que se genere toda la documentación necesaria para que el proceso cumpla con los estándares definidos por la norma, también está conformada por la gestión de cambios y la gestión de capacidad.

- **Protección contra códigos maliciosos:** Define los lineamientos para proteger las estaciones de trabajo de los usuarios finales y los servidores contra cualquier ataque informático y establece las reglas en las cuales debe operar estos controles y cómo actuar frente a cualquier sospecha de amenaza.

- **Copias de respaldo:** Establece los lineamientos para realizar las copias de seguridad a los servidores de la organización, así mismo su frecuencia, también se incluyen controles de prueba de integridad de los respaldos, pues es necesario verificar que estos funcionarán correctamente en el caso de requerir realizar una recuperación de emergencia, también se definen los responsables por garantizar que los respaldos se están realizando correctamente según la programación establecida.

- **Registro de actividad y supervisión:** Todos los servidores deben tener habilitada la función de logs del sistema para verificar las acciones realizadas por los administradores del servidor, esto es fundamental ya que en el caso de un ataque informático se debe recopilar la información del ataque para mitigar este y presentar los recursos legales que sean

considerados por la organización, además, se define el tiempo de retención, el cual es de dos (2) años.

- **Control de software de explotación:** Tanto los usuarios finales como los administradores de los sistemas tienen prohibido la instalación de aplicaciones de intrusión en los sistemas, así mismo, en los servidores está prohibido la instalación de aplicaciones/herramientas sin la previa autorización por medio del formato de Control de Cambios.

- **Gestión de la vulnerabilidad técnica:** Hace referencia al procedimiento PRIN002 – GESTIÓN DE VULNERABILIDAD TÉCNICA, el cual establece las métricas con la que se realizarán los análisis de vulnerabilidades a los servidores de la organización, esto es con base en el ciclo del Hacking ilustrado en la Fig. 23. Este procedimiento también instaura las herramientas a usar y el cronograma de ejecución.

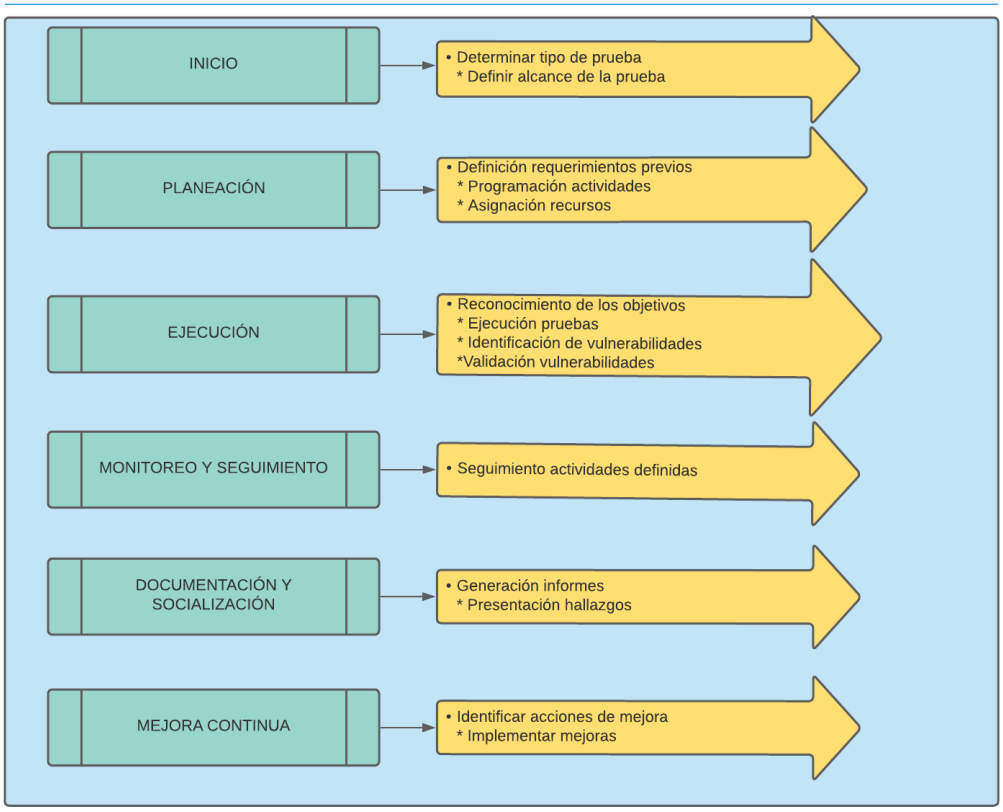

Fig. 23. Metodología pruebas.

- **Consideraciones de las auditorías de sistemas de información:** Para los administradores de los servicios y servidores se definen usuarios que no tengan permisos superiores, estos deben realizar sus funciones con los mínimos privilegios y elevarlos solo en el momento que sea necesario, por ende, en cualquier momento el proceso de Seguridad Informática podrá auditar al personal de TI para validar que estén realizando sus tareas con los permisos asignados y que los servidores no tengan usuarios creados con permisos diferentes.

9.2 Seguridad Comunicaciones

La administración de la red de la organización se encuentra segmentada de acuerdo con los roles de los especialistas del área de Tecnología Informática de la siguiente forma:

- **Conectividad:** Responsable por garantizar la operación del servicio a nivel de capa física y capa de aplicación del modelo OSI, entre estos está (Switches, Routers, Cableado Estructurado, Energía, UPS, ISP, Firewall, SDWAN, MPLS, Wifi, LAN […])

- **Operaciones:** Responsable por garantizar la operación de los servidores a nivel de aplicación y sistema operativo, también es responsable por gestionar el acceso seguro y eficiente de los usuarios a la red.

- **Microinformática:** Deberá garantizar que los equipos de cómputo asignados a los usuarios tienen todos los controles de seguridad definidos, tales como software antivirus, parches de seguridad, software licenciado, sistema operativo actualizado […], también, deberá garantizar que los usuarios que tienen asignados equipos portátiles cuentán con el disco cifrado y con guaya de seguridad para asegurarlo.

- **Seguridad:** Deberá velar porque la política de seguridad sea cumplida en cada uno de los procesos y garantizar un funcionamiento seguro de los sistemas apoyando de manera transversal cada uno de estos, también deberá garantizar que las vulnerabilidades en la red son mitigadas de forma eficiente.

- **Dirección:** Responsable por gestionar los recursos tanto económicos como humanos para poder realizar una gestión óptima de la red, también, deberá velar porque cada uno de los procesos cumpla con su función de acuerdo con la política de seguridad.

Cada uno de los responsables de los procesos debe garantizar que cuenta con los procedimientos actualizados para realizar sus funciones de administración y gestión.

El área de Tecnología Informática es responsable por aplicar los controles necesarios, que permitan tener un adecuado nivel de seguridad en la red y de la información que fluye a través de esta. A continuación, se mencionan las consideraciones más importantes:

- Todos los dispositivos de red deben contar con acceso mediante contraseña, esta debe ser creada con base en la política PLIN018 – GESTIÓN DE CONTRASEÑAS, mientras sea posible, usar doble factor de autenticación.
- Los dispositivos de red deben contar con los últimos parches de seguridad aplicados
- Generar un informe de estado de la red SDWAN de forma trimestral y compartirlo con el equipo de trabajo en busca de medidas correctivas o preventivas que sea necesario aplicar.
- Las conexiones con terceros deben cumplir la política PLIN011 – RELACIÓN CON PROVEEDORES.
- Las conexiones remotas serán únicamente por medio de VPN SSL con el usuario y contraseña asignado, este usuario estará sujeto a los controles de acceso aplicados a nivel de Directorio Activo y Firewall.
- Se Implementan mecanismos de control como: Firewall, IPS, IDS, WAF, SDWAN, EMS (Forticlient), Cylance, Filtrado de contenido […]
- Se verifica que las conexiones desde la red, con las redes externas se encuentren protegidas por un firewall e implementar las reglas apropiadas para filtrar el tráfico permitido entre dichas redes.

- Las direcciones lógicas internas, configuraciones e información de los sistemas de comunicación y cómputo deben ser tratadas como información reservada.
- El líder de Conectividad es el único responsable de realizar cambios en la configuración de los equipos de comunicaciones. Se coordinará con el proveedor de los canales y el proveedor de Datacenter las actividades necesarias cuando se requiera nuevas instalaciones o validaciones en sitios por temas de incidentes de conectividad.
- Los centros de datos cuentan con controles de acceso biométricos a los cuales solo puede acceder personal autorizado.
- En caso de ser requerido, los especialistas realizarán el monitoreo de los canales de comunicación.
- Se segmenta lógicamente la red e implementan mecanismos de control perimetral y de acceso, de tal forma que los usuarios de la red mantienen una independencia sobre las mismas.
- En la selección de proveedores de comunicaciones debe tener en cuenta compañías debidamente establecidas, con licencia de operación y una amplia trayectoria en el mercado, deben demostrar buenas prácticas de seguridad de la información.
- Cuando aplique, se exige a los terceros contratados, la firma del acuerdo de confidencialidad que se establece en el apartado.
- El área de Tecnología Informática se reserva el derecho de otorgar el ingreso a sus sistemas de información, a los colaboradores o terceros, previa autorización.
- Los accesos remotos con los que cuenta el área de Infraestructura Tecnología Informática son de uso exclusivo para la operación de las sedes y labores netamente de administración y gestión de la plataforma tecnológica.
- Las conexiones con los sistemas y redes deben realizarse a través de los equipos portátiles asignados para la operación del servicio. Está prohibido el uso de equipos personales para realizar estas conexiones.
- Los accesos remotos son exclusivamente para la gestión de plataformas y/o labores de control para el personal autorizado, toda conexión es monitoreada y almacenada en los logs de los dispositivos.

Cualquier actividad diferente a la establecida, que sea realizada por los accesos remotos y cuya consecuencia no sea propia de la actividad desarrollada por la persona que realizó la conexión, será responsabilidad del usuario a quién se asignó el acceso.

10 Desarrollo y Mantenimiento de Sistemas de Información

Socia BPO no realiza sus desarrollos de Software in house, todos estos son proyectos asignados a sus diferentes proveedores, por lo que este dominio se controla a través de la política PLIN011 – RELACIÓN CON PROVEEDORES, adicionalmente, todos estos deben firmar los respectivos acuerdos de confidencialidad antes de acceder a la información de la organización.

A los proveedores que tienen relación comercial con Socia BPO se les exige el cumplimiento de buenas prácticas en el desarrollo, testing, despliegue y publicación de las aplicaciones que desarrollen.

11 Relación con Proveedores

La política de Relación con Proveedores describe los lineamientos necesarios para que durante la prestación de sus servicios se cumpla con la custodia de la información, esto, además, está sustentando por un acuerdo de confidencialidad que garantice que el cumplimiento de la ley.

11.1 Principios Generales de Seguridad

El proveedor de servicios proporcionará a Socia BPO, siempre que se requiera, la relación de personas, perfiles, funciones y responsabilidades asociados al servicio prestado, e informará de cualquier cambio (alta, baja, sustitución o cambio de funciones o responsabilidades) que se produzca en dicha relación.

Los proveedores de servicios deberán asegurar que todo su personal tiene la formación y capacitación apropiada para el desarrollo del servicio provisto, tanto a nivel específico en las

materias correspondientes a la actividad asociada a la prestación del servicio, como en materia de seguridad de la información.

Como mínimo, los proveedores de servicios deberán asegurarse de que todo el personal asociado al servicio conoce y se compromete a cumplir lo recogido en esta política.

Confidencialidad de la Información

Toda información, documentación, programas y/o aplicaciones, métodos, organización, estrategias de negocio y actividades relacionadas con el core tecnológico, a las que tenga acceso los proveedores de servicios con objeto de realización del servicio serán considerados información reservada, en función de lo cual, el acceso, intercambio y tratamiento de dicha información, se realizará siempre de acuerdo con las finalidades previstas descritas en el contrato de prestación de servicios y acuerdo de confidencialidad y manteniendo el correspondiente deber de secreto durante la duración del servicio y después de que finalice la relación.

Todos los recursos e información a la que haya podido tener acceso o que haya sido necesaria elaborar, modificar o copiar para el correcto desempeño del servicio serán devueltos a la finalización de este.

11.2 Propiedad Intelectual

Se garantizará el cumplimiento de las restricciones legales al uso del material protegido por la normativa de propiedad intelectual. Los proveedores de servicios únicamente podrán utilizar material autorizado para el desarrollo de sus funciones.

Queda estrictamente prohibido el uso de programas informáticos sin la correspondiente licencia en los sistemas de información de Socia BPO.

11.3 Intercambio de Información

Cualquier tipo de intercambio de información que se produzca entre Socia BPO y los proveedores de servicios se entenderá que ha sido realizado dentro del marco establecido por el

contrato de prestación de servicios correspondiente, de modo que dicha información no podrá ser utilizada fuera de dicho marco ni para otros fines.

La distribución de información ya sea en formato electrónico o físico se realizará mediante los recursos determinados en el contrato de prestación de servicios para tal cometido y para la finalidad exclusiva de facilitar las funciones asociadas a dicho contrato.

Se prohíbe explícitamente:

- La transferencia de información protegida a terceras partes no autorizadas.
- La transmisión o recepción de toda clase de material pornográfico, de naturaleza sexual explícita, declaraciones discriminatorias raciales y cualquier otra clase de declaración o mensaje clasificable como ofensivo o ilegal.
- La transmisión o recepción de información sensible, salvo que la comunicación electrónica esté cifrada y el envío esté autorizado por escrito.

11.4 Uso apropiado de los recursos corporativos

Los recursos corporativos a los que tengan acceso los proveedores de servicios serán utilizados exclusivamente para cumplir con las obligaciones y propósitos de la provisión del servicio. Bajo ningún concepto podrán ser utilizados para actividades no relacionadas con el propósito del servicio o para la comisión de actividades que pudieran ser consideradas ilícitas, como daños contra la propiedad intelectual de terceros, incumplimientos de la normativa de protección de datos entre otros.

Los proveedores de servicios se comprometen a utilizar los recursos corporativos a los que tenga acceso de acuerdo con las políticas de seguridad. Con el fin de velar por el correcto uso de los mencionados recursos, Socia BPO podrá implementar los mecanismos de control y auditoría que considere oportunos, ya sea de forma periódica o cuando por razones específicas de seguridad o del servicio resulte conveniente.

En caso de apreciar que algún proveedor de servicios, o su personal, utiliza incorrectamente recursos o información, se le comunicará tal circunstancia al responsable por parte del proveedor para que realice las acciones oportunas.

Socia BPO se reserva el derecho de ejercer las acciones que legalmente le amparan para la protección de sus derechos. Cualquier fichero introducido en la red de Socia BPO o en cualquier equipo conectado a ella a través de soportes automatizados, internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas normas y en especial, las referidas a propiedad intelectual, protección de datos de carácter personal y control de Malware.

Se prohíbe expresamente:

- Introducir en los sistemas de información o la red contenidos obscenos, amenazadores, inmorales u ofensivos.
- Introducir voluntariamente en la red cualquier tipo de Malware, dispositivo lógico, dispositivo físico o cualquier otro tipo de secuencia de órdenes que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los recursos informáticos.
- Todo el personal con acceso a la red tendrá la obligación de utilizar los programas antivirus actualizados.
- Obtener sin autorización explícita otros derechos o accesos distintos a aquellos que les haya asignado.
- Acceder sin autorización explícita a áreas restringidas de los sistemas de información.
- Distorsionar o falsear los registros “log” de los sistemas de información.
- Descifrar sin autorización explícita las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos informáticos. Poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros usuarios, ni dañar o alterar los recursos informáticos.
- Destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos con información protegida.

11.5 Requisitos de Seguridad para los Dispositivos

Todos los dispositivos con acceso a información de Socia BPO, independientemente de la propiedad de estos, deberán cumplir con las políticas de seguridad.

Se tendrán en cuenta las siguientes consideraciones:

- El acceso a los sistemas deberá realizarse siempre de forma autenticada, al menos mediante la utilización de un identificador personal y una contraseña asociada.
- Los dispositivos deberán permanecer actualizados con la última versión disponible de parches de seguridad para el software y sistema operativo instalado.
- Los dispositivos deben contar con un sistema de protección antimalware instalado, activo y actualizado a su última versión disponible.
- Debe activarse el bloqueo de pantalla para que se ejecute a los 10 minutos de inactividad. El desbloqueo deberá conllevar el uso de contraseñas, patrones de desbloqueo o mecanismos equivalentes, que garanticen que el dispositivo no podrá ser utilizado por un usuario no autorizado.
- Los dispositivos no dispondrán de ninguna herramienta o ficheros contrarios a la política de seguridad que pueda interferir con el software corporativo. Este punto incluye, aquellos que traten de descubrir información distinta de la del propio usuario o realizar accesos no autorizados, como por ejemplo sniffers, herramientas de escaneo de redes, descubrimiento de contraseñas, entre otros.

11.6 Comunicación de Incidentes de ciberseguridad

Los proveedores de servicios se comprometen a comunicar de manera inmediata cualquier incidente de ciberseguridad, debilidad o amenaza (observada o sospechada) que detecte en los sistemas de información o que haya podido afectar la información propiedad de Socia BPO o de sus clientes al correo definido para tal fin, o a través del responsable del servicio.

12 Gestión de Incidentes

Nivel de prioridad: Los niveles de prioridad son definidos dependiendo del valor o la importancia que estos tienen dentro de la entidad y del proceso que soporta en los sistemas afectados.

TABLA XIII
NIVEL DE PRIORIDAD INCIDENTES

Nivel criticidad	Valor	Definición
Inferior	0.10	Sistemas no críticos, como estaciones de trabajo de usuarios con funciones no críticas.
Bajo	0.25	Sistemas que apoyan a una sola dependencia o proceso de una entidad.
Medio	0.50	Sistemas que apoyan más de una dependencia o proceso de la entidad.
Alto	0.75	Sistemas pertenecientes al área de tecnología informática y estaciones de trabajo de usuarios con funciones críticas.
Superior	1.00	Sistemas críticos.

Impacto Actual: depende de la cantidad de daño que ha provocado el incidente en el momento de ser detectado.

Impacto Futuro: Depende de la cantidad de daño que pueda causar el incidente si no es contenido, ni erradicado.

TABLA XIV
IMPACTO INCIDENTES

Nivel impacto	Valor	Definición
Inferior	0.10	Impacto leve en uno de los componentes de cualquier sistema de información o estación de trabajo.
Bajo	0.25	Impacto moderado en uno de los componentes de cualquier sistema de información o estación de trabajo.
Medio	0.50	Impacto alto en uno de los componentes de cualquier sistema de información o estación de trabajo.
Alto	0.75	Impacto moderado en uno o más componentes de más de un sistema de información.
Superior	1.00	Impacto alto en uno o más componentes de más de un sistema de información.

Con las variables definidas se realiza una operación matemática para obtener el nivel de prioridad con la que debemos gestionar el incidente.

Nivel de prioridad = (impacto actual * 2.5) + (impacto futuro * 2.5) + (criticidad del sistema * 5)

TABLA XV
PRIORIDAD INCIDENTES

Nivel de prioridad	Valor
Inferior	00.00 – 02.49
Bajo	02.50 – 03.74
Medio	03.75 – 04.99
Alto	05.00 – 07.49
Superior	07.50 – 10.00

Con base en los resultados obtenidos en la tabla de nivel de prioridad se define un tiempo de atención máximo de incidentes, con el fin de atender adecuadamente estos de acuerdo con su criticidad e impacto.

Estos tiempos son los máximos soportados para atender los incidentes de acuerdo con su prioridad.

TABLA XVI
TIEMPO DE RESPUESTA INCIDENTES

Nivel prioridad	Tiempo de respuesta
Inferior	36 horas
Bajo	24 horas
Medio	12 horas
Alto	8 horas
Superior	4 horas

Todo incidente dentro de la organización deberá contar con el siguiente flujo para su gestión:

- Detección y análisis del incidente
- Contención, erradicación y recuperación
- Ejecución plan definido ya sea por el comité técnico o por el comité de Seguridad de la Información
- Monitoreo del incidente
- Generar informe del incidente en el formato FTIN009 – GESTIÓN DE INCIDENTES y comunicarlo a las partes interesadas

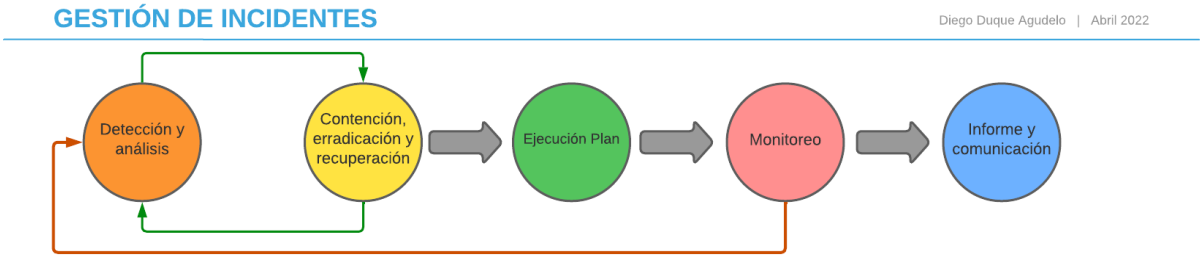

Fig. 24. Gestión de incidentes.

Todo el personal, proveedores y terceros son responsables por informar acerca de los incidentes de seguridad que sufran mientras tienen relación con la organización, de omitir información, la empresa podrá tomar las medidas que crea pertinentes.

Todos los incidentes reportados deben tener como finalización una serie de lecciones aprendidas que lleven a una serie de acciones concretas que permitan la corrección del agujero de seguridad que permitió la materialización del incidente.

Los agujeros de seguridad que provocan los incidentes deben ser identificados de forma proactiva para evitar una filtración de información o una no disponibilidad en los servicios de la organización.

13 Gestión de la Continuidad del Negocio

Para definir qué activos se deben incluir en el plan de Continuidad del Negocio se realiza una matriz BIA, la cual busca dar entendimiento de cuáles son los activos más críticos para el

negocio para que estos sean priorizados, así mismo, se evalúa la criticidad de los sistemas de información, el resultado de esta matriz son proyectos que busquen garantizar la disponibilidad de los sistemas de información críticos ante cualquier desastre que se pueda presentar, ya sea por ataques informáticos, desastres naturales o robo de los equipos.

A continuación, se presentan las tablas que permiten realizar el análisis cualitativo de los activos

Las TABLAS XVII y XVIII determinan las necesidades temporales (RTO) y limitaciones de pérdida de datos (RPO) para proceso o actividad, desde el punto de vista del negocio.

TABLA XVII
ESTIMACIÓN RTO

1. TABLA PARA ESTIMAR EL RTO	
VALOR	**DESCRIPCIÓN**
1	La actividad o el proceso requiere alta disponibilidad (100%).
2	La actividad o el proceso no puede estar interrumpida más de 8 horas.
3	La actividad o el proceso no puede estar interrumpida más de 24 horas.
4	La actividad o el proceso no puede estar interrumpida más de 72 horas.
5	Otros requisitos menos restrictivos que los indicados previamente.

TABLA XVIII
ESTIMACIÓN RPO

2. TABLA PARA ESTIMAR EL RPO	
VALOR	**DESCRIPCIÓN**
1	La actividad o el proceso requiere disponer del 100% de los datos.
2	La actividad o el proceso toleran la pérdida de los datos generados o modificados en las últimas 4 horas.
3	La actividad o el proceso toleran la pérdida de los datos generados o modificados en las últimas 8 horas.
4	La actividad o el proceso toleran la pérdida de los datos generados o modificados en las últimas 24 horas.
5	Otros requisitos menos restrictivos que los indicados previamente.

Las TABLAS XIX y XX determinan las capacidades de los sistemas en cuanto al tiempo de recuperación (RTO) y la política de copias (RPO).

TABLA XIX
CAPACIDAD DE SISTEMAS RTO

3. TABLA PARA ESTIMAR LA CAPACIDAD DE SISTEMAS EN TÉRMINOS DE RTO

VALOR	DESCRIPCIÓN
1	Los servicios y herramientas TIC de los que dependen la actividad o el proceso disponen de una configuración de alta disponibilidad (100%).
2	Es posible recuperar los servicios y herramientas TIC de los que dependen la actividad o el proceso en un tiempo inferior a 8h.
3	Es posible recuperar los servicios y herramientas TIC de los que dependen la actividad o el proceso en un tiempo inferior a 24h.
4	Es posible recuperar los servicios y herramientas TIC de los que dependen la actividad o el proceso en un tiempo inferior a 72h.
5	No existen medios que garanticen la recuperación de los servicios y herramientas TIC de los que dependen la actividad o el proceso en un tiempo inferior a los indicados y/o el tiempo de recuperación no está acotado.

TABLA XX
CAPACIDAD DE SISTEMAS RPO

4. TABLA PARA ESTIMAR LA CAPACIDAD DE SISTEMAS EN TÉRMINOS DE RPO	
VALOR	**DESCRIPCIÓN**
1	Los servicios y herramientas TIC de los que dependen la actividad o el proceso disponen de una configuración de alta disponibilidad de datos (100%).
2	La solución y política de copias existente garantiza que, a lo sumo, se perderán los datos generados o modificados en las últimas 4 h.
3	La solución y política de copias existente garantiza que, a lo sumo, se perderán los datos generados o modificados en las últimas 8 h.
4	La solución y política de copias existente garantiza que, a lo sumo, se perderán los datos generados o modificados en las últimas 24 h.
5	No se realizan copias de seguridad.

14 Cumplimiento

Todos los empleados de la organización y cuando sea pertinente proveedores, deberán recibir concientización, entrenamiento y formación adecuada y actualizaciones regulares en políticas y procedimientos organizacionales, relevantes para su función laboral.

- La Gerencia de cada organización debe comprometerse con la formación y sensibilización en seguridad de la información de todos sus colaboradores, asignando tiempo y recursos económicos para tal fin.
- Cada año se debe reforzar en los colaboradores el conocimiento y el cumplimiento de las obligaciones aplicables de seguridad de la información contenida en las políticas, normas y contrato laboral.

- Las políticas deben estar accesibles para todos los colaboradores de la organización en la INTRANET corporativa.
- Cada año se deberán realizar encuestas que reflejen el conocimiento actual de los colaboradores sobre sus responsabilidades en el cumplimiento de las políticas de seguridad de la información.
- Cada mes se publicará un poster en carteleras digitales o físicas sobre una política de seguridad.
- En la inducción o reinducción se debe incluir políticas específicas de seguridad de la información como:
  - Política de Escritorio Limpio
  - Confidencialidad de la información
  - Uso Adecuado de Activos
  - Canales de notificación de incidentes de seguridad
  - Uso de contraseñas seguras
  - La responsabilidad de los colaboradores y proveedores de sus propias acciones u omisiones en la protección de la información.

- Dos veces por mes se enviarán boletines de seguridad con temas de interés sobre seguridad de la información a los colaboradores de la organización.
- Dos veces por año se deberá ofrecer capacitaciones a los Colaboradores sobre los riesgos en el mundo digital, ofrecida por expertos en el tema de Seguridad de la información.
- Dos veces por año se deberá ofrecer capacitaciones a los directivos de la organización sobre los riesgos a los que están expuestos por la criticidad de su cargo y la responsabilidad que tienen frente a la seguridad de la información.
- Cada 3 meses se deberán ofrecer capacitaciones internas y/o externas al personal de TI para reforzar su conocimiento en la detección y gestión de incidentes de seguridad.
- Las capacitaciones deberán ser grabadas y publicadas en STREAM para que sea de fácil acceso para los colaboradores que deseen reforzar sus conocimientos.

14.1 Sensibilización seguridad de la información

Se realizarán campañas de concienciación sobre seguridad de la información en la empresa, el fin de estas campañas será detectar las falencias en cuanto a madurez del conocimiento de los colaboradores en cuanto a la seguridad de la información.

- Los talleres de concienciación podrán ser realizados por personal interno o externo a la organización
- Antes de iniciar los talleres de concienciación se deberán realizar pruebas controladas para no afectar la producción de los colaboradores ni de la organización.
- Los talleres se deben realizar en ambiente totalmente controlados.
- Los talleres de concienciación se podrán realizar a toda la organización o por empresas, dependiendo del acuerdo al que se llegue con la gerencia para realizar estas actividades.
- Los talleres de concienciación se realizan una vez al año, en el cual se podrán ir desplegando las actividades en lo corrido de este.

Las actividades de sensibilización que se realizarán serán las siguientes:

- Ataque dirigido por Phishing, suplantando un sitio web que capture únicamente el usuario y la contraseña del usuario que acceda al sitio fraudulento.
- Ataque con memoria USB “Contaminada”. Se despliegan USB contaminadas en algunos sectores de la organización, si un usuario accede a esta se desplegará un mensaje informativo advirtiéndole del peligro que supone lo que acaba de hacer.
- Se enviarán boletines recordando la importancia de no confiar en fuentes desconocidas.
- Se enviará una encuesta para reforzar el conocimiento en seguridad de la información.

Fig. 25. Imagen corporativa Institute of Electrical and Electronics Engineers (IEEE)

Nota: fuente https://www.ieee.org/ Esta entidad edita y normaliza la presentación de documentos científicos en el área de ingenierías.

Fig. 26. Logo Universidad de Antioquia

Nota. Fuente http:/www.udea.edu.co

VII. CONCLUSIONES

La identificación de brechas de seguridad permitió evidenciar a la gerencia la carencia de políticas, procedimientos y manuales para la correcta gestión de la información de los clientes, empleados y socios comerciales.

La gestión de riesgos realizada en la organización estableció las bases para la mejora continua del Plan de Seguridad Informática. Se resalta una alta probabilidad e impacto de la materialización de amenazas relacionadas con abuso de información privilegiada y actos no autorizados, ataques internos, ataques externos, intrusión física y/o robo, errores y omisiones, fallos en el sistema y en el medio ambiente, mientras no se siga con el Plan de Seguridad Informática.

De acuerdo con el análisis realizado de riesgos y controles proporcionados por la ISO-IEC 27001 a través de sus 14 dominios, se estableció la ejecución de las siguientes actividades:

- Definición y comunicación de Políticas de Seguridad.
- Creación de MZ para la granja que servidores para minimizar la superficie de ataque.
- La implementación de un Email Security Gateway para gestionar los riesgos inherentes en los correos electrónicos.
- La contratación de una auditoría por una empresa experta en seguridad informática.
- La contratación de capacitaciones de sensibilización para todo el personal, directivos y área de TI en gestión de riesgos.
- Cifrado de equipos de cómputo de los colaboradores de toda la compañía con BitLocker.
- Realización de Hacking Ético a los servidores de la compañía en busca de debilidades que puedan poner en riesgo la información y las operaciones de la organización.
- La implementación de Software antivirus para los servidores que aumenten su protección.
- Implementación de un sistema WSUS para garantizar que todos los nodos se encuentren con los últimos parches de seguridad.

La definición, asignación y comunicación de las responsabilidades tienen un papel trascendental en el correcto funcionamiento del PSI, pues, es importante establecer el compromiso de todos los miembros con la protección de la información, delimitar las actividades del personal dentro de la organización, alinear los procesos y estándares, mejores prácticas y contribuir al establecimiento de directrices de seguridad de la información.

El presente proyecto fija las bases para la implementación del PSI en Socia BPO. El proceso está arraigado en la mejora continua, por lo tanto, nunca concluye, para que esto sea posible es importante contar con la participación activa de todos los implicados (gerentes, personal, clientes proveedores […]) en la seguridad y tratamiento de la información.

REFERENCIAS

[1] K. Terrell Hanna, “Gap Analysis,” [En línea]. Disponible en: https://cutt.ly/oLUcFhD.

[2] ITservice, “ISO 27001: Una breve historia de la norma” [En línea]. Disponible en: https://cutt.ly/wLUcCfz .

[3] El Economista. “Ciberataques le cuestan 8 mil millones de dólares a empresas a nivel global” *El Economista*, 2021, [En línea]. Disponible en https://cutt.ly/xLUcBnM .

[4] L. López. “El 60% de las empresas que sufren un ciberataque se ven obligadas a cerrar” *El Mundo*, 2021, [En línea]. Disponible en: https://cutt.ly/gLUc1X7 .