DISEÑO DE UN MODELO DE SEGURIDAD INFORMÁTICA BASADO EN LA GESTIÓN DE INCIDENTES PARA EL ÁREA DE SISTEMAS Y TECNOLOGÍA DE LA COMPAÑÍA GRUPO TX

OSCAR JAVIER DELGADO VILLAMIL

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN DE SEGURIDAD INFORMÁTICA
BOGOTÁ, COLOMBIA
2020

DISEÑO DE UN MODELO DE SEGURIDAD INFORMÁTICA BASADO EN LA GESTIÓN DE INCIDENTES PARA EL ÁREA DE SISTEMAS Y TECNOLOGÍA DE LA COMPAÑÍA GRUPO TX

OSCAR JAVIER DELGADO VILLAMIL

Proyecto de grado aplicado para la obtención del título de:
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Director Trabajo de Grado
Ingeniero Martín Camilo Cancelado

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN DE SEGURIDAD INFORMÁTICA
BOGOTÁ, COLOMBIA
2020

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Bogotá. D.C, 28 de mayo de 2020

A mi esposa

Que siempre ha estado apoyándome incondicionalmente en este proceso y alentándome a ser un mejor ser humano, a mis familiares y amigos por la confianza depositada en mí.

Oscar Delgado

AGRADECIMIENTOS

Agradezco a Dios por permitirme continuar con mis estudios de posgrado. Agradezco a mi esposa por la paciencia, por la colaboración, que necesitaba, por estar allí en los momentos más complejos para motivarme a seguir con el objetivo de terminar la especialización en seguridad informática. Agradezco a mis padres que desde siempre me han apoyado en todos mi sueños y proyectos.

RESUMEN

Las probabilidades de recibir cualquier tipo de ataques cibernéticos es un problema que ha venido afectado a todas las organizaciones públicas o privadas, esto conlleva a la implementación de políticas de seguridad efectivas capaces de minimizar los riesgos existentes. El desafío es bastante complejo debido a que involucra la seguridad física, lógica y el entrenamiento del talento humano, aun así, es factible superarlo. Por esta razón es importante que las organizaciones tengan implementadas las políticas de seguridad, que sean totalmente claras, aplicables, de conocimiento general y que se exija su cumplimiento a cabalidad.

En el presente proyecto, se realizará un análisis de requerimientos de seguridad informática, para así poder determinar cuáles son las necesidades y con ello poder construir el modelo de tratamiento de incidentes aplicando los respectivos salvaguardas correspondientes al área de sistemas y tecnología de la compañía Grupo TX, tomando como referencia la norma ISO 27001 e ISO 9001, orientada a los objetivos del negocio.

Palabras clave: Confidencialidad, diseño, disponibilidad, información, ISO 9000, ISO 27001, MAGERIT, políticas de seguridad, procedimientos, sistemas y tecnología, vulnerabilidad.

ABSTRACT

The probability of receiving any type of cyber attack is a problem that has affected all public or private organizations, this leads to the implementation of effective security policies capable of minimizing existing risks. The challenge is quite complex because it involves physical security, logic and the training of human talent, even so, it is feasible to overcome it. For this reason, it is important that organizations have security policies in place, that they are totally clear, applicable, of general knowledge and that they are fully enforced.

In this project, an analysis of computer security requirements will be carried out, in order to determine what the needs are and thus be able to build the incident treatment model applying the respective safeguards corresponding to the systems and technology area of the Grupo TX company. , taking as reference the ISO 27001 and ISO 9001 standards, oriented to the business objectives.

Keywords: Confidentiality, design, availability, information, ISO 9000, ISO 27001, MAGERIT, security policies, procedures, systems and technology, vulnerability.

CONTENIDO

Pág.

LISTA DE TABLAS

LISTA DE FIGURAS

Pág

LISTA DE ANEXOS

1. INTRODUCCIÓN

Al tiempo que avanza la tecnología de la información, también evolucionan los tipos de amenazas, por lo que es necesario tener en cuenta qué medidas deben tomarse para mitigar los posibles riesgos a los que está expuesta la información de una organización, con el fin de realizar un tratamiento correcto de incidentes, debido a que la información debe tratarse como el activo más importante que se puede tener y, al mismo tiempo, el más vulnerable si no hay planes de acción y contingencia. Además, un ataque a la información primaria y los procesos comerciales pueden detener todas las operaciones normales, desencadenando problemas de todo tipo.

Teniendo en cuenta lo anterior es importante que las empresas públicas o privadas, tengan un modelo de política de seguridad que sea suficientemente claro y aplicable a cada negocio en particular, y que todos los usuarios involucrados deben conocerlas y cumplirlas.

En este documento, se realizará un análisis de los requisitos de seguridad informática, de acuerdo con las características del negocio, para determinar las necesidades y así desarrollar un modelo de tratamiento de incidentes aplicando las salvaguardas relevantes en el área de sistemas y tecnología de la compañía Grupo TX. Como información importante es posible decir que en 2018 se realizó la última actualización de la plataforma tecnológica, con el fin de mejorar su desempeño, lo que resultó en una mayor eficiencia y así poder aumentar la confiabilidad y disponibilidad de recursos tecnológicos.

Para desarrollar el modelo, se utilizarán como referencia los estándares ISO 27001 e ISO 9001, gracias a ellos se garantiza que se cumplen los requisitos mínimos para lograr un buen diseño del modelo de seguridad informática propuesto, garantizando así la preservación de la confidencialidad, integridad y disponibilidad de la información dentro de la organización. Esto mejorará el sistema de gestión actual. Además, el proceso y el procedimiento de gestión de incidentes con anexos como formatos, políticas de seguridad y cronograma se dejarán documentados para tener evidencia del diseño y la ejecución del modelo.

2. DISEÑO DE UN MODELO DE SEGURIDAD PARA EL ÁREA DE SISTEMAS Y TECNOLOGÍA DE LA COMPAÑÍA GRUPO TX

2.1 PLANTEAMIENTO DEL PROBLEMA

En la actualidad el área de Sistemas y Tecnología de Grupo TX, de acuerdo con el análisis realizado en la compañía, se identificaron los siguientes inconvenientes:

Lentitud en el servicio prestado a los usuarios finales, esto debido a la falta de un sistema de apoyo y atención a servicios adecuados, lo que permitiría mantener un nivel de servicio óptimo en el uso de la tecnología de la información, soporte de hardware inadecuado, falta de reglas específicas sobre el uso de TI en la organización, alineadas con los estándares internacionales, baja disponibilidad de TI, falta de conciencia y capacitación de los funcionarios, los incidentes no ingresan siempre por donde debería ser el primer punto de contacto, varios casos han sido atendidos directamente por el personal de soporte sin ni siquiera ser registrados, las responsabilidades y roles no están claramente definidos originando en diversos casos los colaboradores ejecuten tareas que no le corresponden con respecto a la atención de un incidente, entre otros.

2.2 DEFINICION DEL PROBLEMA

¿Cómo debe diseñarse el modelo de seguridad informática para el área de sistemas y tecnología y que los usuarios del área lo utilicen como una herramienta útil, optimizando la gestión de incidentes sin interrumpir sus tareas cotidianas y que se garantice la buena gestión de la información y los recursos?

3. JUSTIFICACION

La información de una organización es el activo más vital e importante que posee, y por ello debe ser custodiada, implementando políticas de seguridad eficaces y eficientes, pero a pesar de los grandes esfuerzos realizados por organizaciones públicas y privadas, día a día se ven afectados por diferentes ataques cibernéticos, por lo que muchos esfuerzos en las áreas de Tecnología siempre buscan mejorar su infraestructura de seguridad de la información, con el fin de evitar que estos actos maliciosos se produzcan.

Cuando ocurren incidentes de seguridad, es importante que una organización tenga la manera efectiva de responder y en estos casos la velocidad con la que una organización puede reconocer, analizar y responder a un incidente minimizará el daño y reducirá el costo de recuperación.

El presente proyecto de grado está diseñado para el proceso de soporte del área de sistemas y tecnología de la organización, y se llevará a cabo en el período comprendido entre enero y julio de 2020. Se tomará como referencia la teoría de la gestión de riesgos en seguridad informática, ISO 27001 e ISO 9001, adaptándolas a los requisitos de la empresa, específicamente al tratamiento de incidentes, para garantizar la continuidad del negocio y optimizar el tiempo de respuesta del proceso.

El modelo propuesto está orientado al área de sistemas y tecnología de una compañía, pero esto se extiende a otras áreas y procesos debido a que finalmente es uno de los ejes del negocio y es un proceso transversal. Cabe señalar que el sistema no busca la certificación en ISO 27001 o ISO 9001 por parte de la alta

gerencia, pero es un facilitador de negocios y un canal para lograr un cambio cultural dentro de la entidad, generando un impacto positivo en la percepción que tienen sobre los controles aplicados. En los modelos de seguridad de la información, además de garantizar el buen desarrollo del proceso del área de sistemas y tecnología.

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Construir el modelo de seguridad informática requerido para el tratamiento de incidentes de seguridad informática en el área de Sistemas y Tecnología de la compañía Grupo TX, tomando como referencia la norma ISO 27001 e ISO 9001, orientada a los objetivos del negocio.

4.2 OBJETIVOS ESPECÍFICOS

- Elaborar un análisis exhaustivo de la compañía Grupo TX, para identificar los problemas críticos a tratar con respecto a la seguridad de la información.

- Diseñar la caracterización del proceso de gestión del área de sistemas y tecnología, preparando la documentación respectiva.

- Modelar el diseño del procedimiento de gestión de incidentes, que sea coherente con las características y necesidades del negocio.

- Realizar los diseños de la documentación de los componentes básicos del modelo de seguridad informática propuesto, que contiene las políticas de seguridad, el plan de capacitación y los respectivos formatos.

5. MARCO REFERENCIAL

5.1 MARCO TEORICO

La primera entidad de estandarización global fue la BSI (British Standards Institution), responsable de publicaciones como BS 5750 en 1979 (ahora ISO 9001) o BS 7750 de 1992 (ahora ISO 14001), así como BSI BS 7799 da a luz en 1995[1], y su objetivo era difundir un conjunto de buenas prácticas para la gestión de la seguridad de la información. Después de varios años de modificaciones, adiciones y evolución en el tema, se alcanzó el estándar ISO 27001, que fue aprobado y publicado como un estándar internacional en octubre de 2005.

La implementación del modelo de este proyecto se basa en este estándar, que se asemeja al estándar ISO 9001 pero en seguridad informática, esto significa que muchas entidades en todo el mundo han adoptado este estándar y también están certificados en él como un sistema de gestión de seguridad (SGSI) , estas entidades mejoraron significativamente la calidad de los servicios presentados, como es el caso de [2]la Aeronáutica Civil de Colombia, que al implementar un modelo de seguridad informática, hizo posible que todos los usuarios que tienen que interactuar con el modelo, se comprometan con él , por el bien de la entidad y de esta manera podrán implementar políticas claras adaptadas a su estructura.

Es importante tener en cuenta que hay varias formas de tener algún tipo de incidente informático, que puede deberse a un virus informático, un mal manejo de los recursos por parte de los usuarios debido a la falta de capacitación, a un

---

[1] LÓPEZ NEIRA, Agustín y RUIZ SPOHR, Javier. El portal de ISO 27001 en español: Origen. [en línea]. Disponible en: http://www.iso27000.es/index.html [Citado 15 de febrero de 2020]

[2]AERONÁTICA CIVIL. Modelo de seguridad informática [en línea]. Disponible en: http://portal.aerocivil.gov.co/portal/page/portal/Aerocivil_Portal_Intranet/seguridad_informatica/mejore_seguridad_informacion/proteccion_informacion/propiedad_informacion/modelo_seguridad_informatica [citado: 13 de Marzo de 2020]

ataque de denegación de servicio por parte de un tercero, por eso es necesario tener preparación para poder llevar a cabo un tratamiento de incidentes apropiado para mitigar los riesgos que están evolucionando en nuevas amenazas.

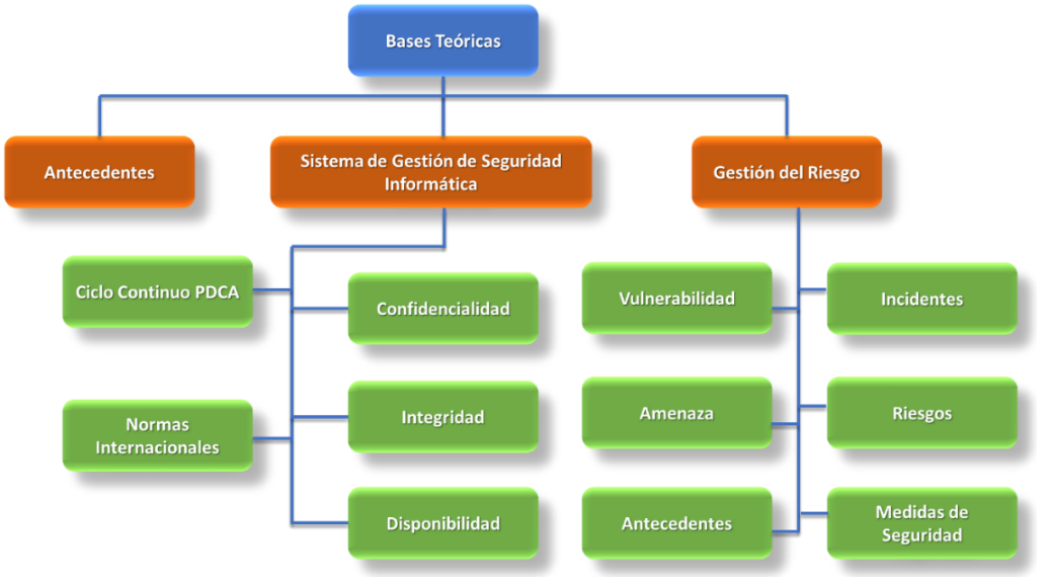
5.2 MARCO CONCEPTUAL

Técnicas o parámetros usados en el desarrollo del trabajo.

El presente proyecto, involucra la teoría de seguridad de la información, para esto, se tomaron conceptos como confidencialidad, integridad, disponibilidad, amenazas, vulnerabilidades e incidentes, así como términos de gestión de calidad para establecer buenos puntos de partida, como lo son las bases teóricas y ser una guía de soporte.

A continuación, en la figura 1, se aprecia el esquema del mapa conceptual para el desarrollo de las bases teóricas.

Figura 1. Bases Teóricas



Fuente: El Autor

5.2.1 Sistema de gestión de seguridad de la información. Es un conjunto de reglas que busca garantizar la confidencialidad, integridad y disponibilidad de la información de una entidad, se abrevia como SGSI, el término se llama "Sistema de Gestión de Seguridad de la Información" (ISMS[3]) en inglés

5.2.1.1 Ciclo continuo Deming PHVA. Es un ciclo de mejora continua, enfocado en cuatro pasos, que no necesariamente debe tener un orden estricto, ya que se adapta específicamente a cada proyecto, en inglés el acrónimo PDCA es el acrónimo de Plan, Do, Check, Act en español PHVA (Planificar, Hacer, Verifcar, Actuar)[4]. Es ampliamente utilizado por los Sistemas de Gestión de Calidad (SGC).

5.2.1.2 Confidencialidad. Se refiere al manejo que se le da a la información para permitir la entrada o negar el acceso no autorizado a la misma.

5.2.1.3 Integridad. Es la preservación y conservación de la información sin ninguna modificación lo que altere su exactitud en todo lo que le concierne al ella.

5.2.1.4 Disponibilidad. Es la capacidad de garantizar el acceso a la información y a los sistemas con los que el usuario interactúa todo el tiempo.

5.2.2 Gestión del riesgo. Es un método para determinar, analizar, evaluar y clasificar el posible riesgo al que está expuesta cualquier entidad, con el fin de implementar posteriormente medidas de seguridad para mitigarlo y controlarlo.

5.2.2.1 Vulnerabilidad. Debilidad que permite a los atacantes comprometer la integridad, disponibilidad y confidencialidad de los sistemas de información.

---

[3] LÓPEZ NEIRA, Agustín y RUIZ SPOHR, Javier. El portal de ISO 27001 en español: Sistema de Gestión de la Seguridad de la Información. [en línea]. Disponible en: http://www.iso27000.es/index.html [Citado 15 de febrero de 2020]

[4] SINGH SOIN, Sarv. Control de calidad total: claves, metodologías y administración para el éxito, McGraw-Hill Interamericana, 2011, pág.94-96

5.2.2.2 Amenaza. Es cualquier evento que pueda causar daños a un sistema de información y que cause pérdidas de cualquier tipo.

5.2.2.3 Incidentes de seguridad. Es cualquier evento no deseado, que puede resultar en la interrupción de los servicios prestados por un sistema informático, se considera que un incidente es la materialización de una amenaza.

5.2.2.4 Riesgos informáticos. Es la incertidumbre que existe debido a la posible materialización de una amenaza que genera daños con respecto a los bienes o servicios informáticos.

5.2.2.5 Medidas de seguridad. Estas son las medidas que se pueden tomar para mitigar un riesgo informático. Sirven para minimizar las vulnerabilidades de un sistema informático, también se conocen como salvaguardas o defensas informáticas.

5.2.2.6 Norma para la seguridad de la información ISO / IEC 27001. Es una norma internacional ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission) que proporciona un marco de gestión de seguridad y sirve como guía para cualquier entidad cumpla los requisitos necesarios para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI)[5], esta norma tiene como objetivos principales:

- Establecer un marco metodológico para un SGSI.
- La adopción de controles para el tratamiento de los riesgos percibidos.

[5] LÓPEZ NEIRA, Agustín y RUIZ SPOHR, Javier. El portal de ISO 27001 en español: la serie 27000. [en línea]. Disponible en: http://www.iso27000.es/iso27000.html#section3b [Citado 15 de febrero de 2020]

- Documentación de políticas, procesos, procedimientos, controles y tratamiento de riesgos.
- Identificación y asignación de responsabilidades y roles al nivel apropiado.
- Seguimiento y revisión de controles y riesgos residuales.
- Generación y preservación de evidencia.
- Tratamiento de incidentes de seguridad.
- Revisión y mejora continua del SGSI.
- Gestión de riesgos.

Este estándar se propone bajo el enfoque metodológico ya mencionado. Plan de Deming del ciclo - Hacer - Verificar - Actuar (PHVA) o en inglés PDCA.

5.2.2.7 Norma para la gestión de calidad ISO 9001: 2008. La norma internacional ISO 9001: 2008 para Gestión de calidad y garantía de calidad contiene las pautas genéricas para la aplicación de las normas ISO 9001, ISO 9002 e ISO 9003[6]. Las siguientes son las cuatro facetas de calidad según este estándar:

- Calidad debido a la definición de las necesidades del producto.
- Calidad debido al diseño del producto.
- Calidad debido al cumplimiento del diseño del producto.
- Calidad debido al soporte del producto (servicio).

5.2.2.8 MAGERIT. Es el acrónimo de "Metodología de análisis y gestión de riesgos de los sistemas de información de las administraciones públicas".
Es una metodología pública desarrollada por el Consejo Superior de Tecnología de la Información (CSI), que es un órgano del Ministerio de Administración Pública

[6] PEACH, Robert W. Manual de ISO 9000 ed. 3, McGraw-Hill Interamericana, 1999, pág. 37-59.

(MAP), responsable de la preparación, desarrollo y aplicación de la política de información del Gobierno español[7]. Esta metodología se crea con el objetivo de minimizar los riesgos de los sistemas de información y telemática, para ayudar a garantizar la autenticación, confidencialidad, integridad y disponibilidad de los sistemas de información. Por lo tanto, se persigue un doble objetivo:

- Estudiar y analizar los riesgos asociados con un sistema de información con su entorno y contexto.
- Recomendar las medidas necesarias para evitar, reducir o controlar los riesgos analizados.

5.2.2.9 ISM3. Es un modelo de gestión de seguridad de la información alineado con los principios de gestión de calidad de ISO 9001, compatible con ISO 27001 e ITIL y aplicado a los sistemas de gestión de seguridad de la información (SGSI). En este modelo hay diferentes niveles de seguridad[8].

5.3 HIPÓTESIS

5.3.1 Hipótesis Investigativa (Ha). Las empresas que adoptan un modelo de seguridad informática con políticas claras y buena gestión de incidentes consolidan y fortalecen el núcleo del negocio, algo que se refleja en sus resultados.

---

[7] LÓPEZ NEIRA, Agustín y RUIZ SPOHR, Javier. El portal de ISO 27001 en español: análisis de Riesgos. [en línea]. Disponible en: http://www.iso27000.es/herramientas.html#section7b [Citado 18 de febrero de 2020]

[8] LÓPEZ NEIRA, Agustín y RUIZ SPOHR, Javier. El portal de ISO 27001 en español: análisis de Riesgos. [en línea]. Disponible en: http://www.iso27000.es/herramientas.html#section7a [Citado 18 de febrero de 2020]

5.3.2 Hipótesis Nula (Ho). Las empresas que adoptan un modelo de seguridad informática con políticas claras y un buen manejo de incidentes, no logran consolidar y fortalecer el núcleo del negocio, algo que se refleja en sus resultados.

5.3.3 Hipótesis Alternativa (HA). Las empresas que realizan un tratamiento eficaz de sus incidentes informáticos pueden proponer salvaguardas eficientes para lograr sus objetivos misionales.

5.3 VARIABLES

En la tabla 1 de variables, se pueden evidenciar las diferentes variables utilizadas en el proyecto junto con su respectiva abreviatura y descripción.

Tabla 1. Variables

Variables	Abreviatura	Descripción
Sistema de Gestión de Seguridad de la Información	S.G.S.I.	conjunto de normas que busca asegurar la confidencialidad, integridad y disponibilidad de la información de una entidad
Tecnologías de Información	TI	Tecnologías enfocadas a tratamiento de la información
Software	SW	Aplicativos/licencias
Hardware	HW	Equipos Físicos/tangibles
Políticas de Seguridad	P.S.	Conjunto de reglas
Gestión del Riesgo	G.R.	Es un método para determinar, analizar, valorar y clasificar el posible riesgo, para posteriormente implementar medidas de seguridad que permitan controlarlo.
Organización Internacional de Normalización	ISO	Organismo encargado de promover el desarrollo de normas internacionales de fabricación (tanto de productos como de servicios), comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica

Fuente: El Autor

6. MARCO LEGAL

Ley 1273 DE 2009 (MINTIC, 2019)[9]. Mediante el cual se modifica el Código Penal, se crea un nuevo bien legal protegido, llamado "la protección de la información y los datos", y los sistemas que utilizan las tecnologías de la información y las comunicaciones se conservan por completo, entre otras disposiciones.

EL CONGRESO DE COLOMBIA DECRETA:

Artículo 1 Agregue el Código Penal con un Título VII BIS llamado "Protección de información y datos", como sigue:

CAPÍTULO I
De los ataques contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos.

Artículo 269A: Acceso abusivo a un sistema informático. Quien, sin la respectiva autorización o fuera del acuerdo, acceda total o parcialmente a un sistema informático protegido o no con una medida de seguridad, o permanezca dentro de él contra la voluntad de quienes tienen el derecho legítimo de excluirlo, incurrirá en pena de prisión 48 a 96 meses y una multa de 100 a 1,000 salarios mínimos legales vigentes.

Artículo 269B: La obstrucción ilegítima del sistema informático o la red de telecomunicaciones. Cualquier persona que, sin autorización para hacerlo, impida o dificulte el funcionamiento normal o el acceso a los sistemas informáticos, a los datos informáticos contenidos en el mismo, o a una red de telecomunicaciones, incurrirá en prisión de 48 a 96 meses y una multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre y cuando la conducta no constituya un delito punible con una pena superior.

Artículo 269C: Interceptación de los datos informáticos. Quien, sin una orden judicial previa, intercepta los datos de la computadora en su origen, destino o dentro de los sistemas informáticos, o las emisiones electromagnéticas de los sistemas informáticos que los transporta, incurrirá en prisión de 36 a 72 meses.

Artículo 269D: Daños informáticos. Cualquiera no esté autorizado para hacerlo, destruya, dañe, altere, elimine o deteriore los datos de una computadora, o un sistema de procesamiento de información, sus partes o componentes lógicos, incurrirá en prisión de 48 a 96 meses y una multa de 100 a 1,000 salarios mínimos legales vigentes.

Artículo 269E: Utilización de software malicioso. Cualquier persona que, sin previa autorización, trafique, produzca, adquiera, distribuya, envíe, venda, introduzca o elimine software malicioso u otros programas informáticos de efectos nocivos del territorio nacional, incurrirá en prisión de 48 a 96 meses y una multa de 100 a 1,000 salarios mínimos legales vigentes.

Artículo 269F: Infracción de los datos personales. Quien, sin autorización para hacerlo, para su propio beneficio o el de un tercero, obtiene, recopila, resta, ofrece, vende, intercambia, envía, compra, intercepta, divulga, modifica o utiliza, datos personales contenidos en archivos, códigos personales, archivos, bases de datos o medios similares, incurrirán en prisión de 48 a 96 meses y una multa de 100 a 1000 salarios mínimos legales vigentes.

Artículo 269G: Suplantación de identidad de sitios web para la captura de datos personales. Cualquiera que, con un propósito ilícito y sin autorización para hacerlo desarrolle, trafique, venda diseñe, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá de 48 a 96 meses de prisión y una multa

de 100 a 1,000 salarios mínimos legales vigentes, siempre y cuando la conducta no constituya un delito punible con una pena más grave.

Se incurrirá en la misma penalización modificando el sistema de resolución de nombres de dominio DNS, de manera que permita al usuario ingresar una IP diferente en la creencia de que accede a su banco u otro sitio personal o de confianza, siempre que la conducta no constituya un delito punible con una pena más grave.

La pena indicada en los dos párrafos anteriores se agravará entre un tercio y la mitad, si para consumar el agente ha reclutado víctimas en la cadena delictiva.

Artículo 269H: Circunstancias de agravamiento punitivo: Las sanciones impuestas de conformidad con los artículos descritos en este título, se incrementarán de la mitad a las tres cuartas partes si la conducta se comete:

1. En las redes o sistemas informáticos o de comunicaciones oficiales, públicas o del sector financiero, nacionales o extranjeros.
2. Servidor público en ejercicio de sus funciones.
3. Aprovecharse de la confianza depositada por quien posee la información o por quien tuviere un vínculo contractual con este.
4. Revelando contenidos de información en perjuicio de otro.
5. Obteniendo provecho para sí mismo o para un tercero.
6. Con multas terroristas o generando riesgo de la seguridad o defensa nacional.
7. Utilizar como instrumento a un tercero de buena fe.
8. Quien incurra en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por 3 años, una pena de inhabilitación del ejercicio de la profesión relacionada con los sistemas de información procesada con equipos computacionales.

CAPITULO II

De los atentados informáticos y otras infracciones

Artículo 269I: Hurto por medios informáticos y similares. El que, superando medidas de seguridad informática, realiza la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio similar, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecida, incurrirá en las penas establecidas en el artículo 240 de este Código.

Artículo 269J: Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna instrucción informática o artificio similar, consiga la transferencia no autorizada de cualquier tipo de activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en prisión 48 a 120 meses y en una multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción será impuesta a quien ingrese, posea, fabrique, o facilite el programa de computador destinado a la comisión del delito especificado en el inciso anterior, o de una estafa.

Si la conducta descrita en los incisos anteriores tuviese una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad. (MINITIC, s.f.).

---

[9] BOGOTA. CONGRESO DE LA REPUBLICA. Ley 1273. (5, enero, 2009) "Por Medio De La Cual Se Modifica El Código Penal, Se Crea Un Nuevo Bien Jurídico Tutelado -Denominado "De La Protección De La Información Y De Los Datos"· Y Se Preservan Integralmente Los Sistemas Que Utilicen Las Tecnologías De La Información Y Las Comunicaciones, Entre Otras Disposiciones. Diario Oficial. 2009. 1-3 p

7. MARCO ESPACIAL

Grupo TX, es un conjunto de empresas líderes en tecnología con el mayor número de contratos en Latinoamérica, caracterizado por proporcionar soluciones integrales a los gobiernos Federales, Estatales, Institutos Autónomos y Empresas Privadas, en la prestación de servicios con éxito garantizado y comprobado, como software para gestión fiscal, hotelería, construcción y gestión inmobiliaria, digitalización, administración y custodia de documentos, catastro y georreferenciación, cobro de cartera, entre otros. La compañía se encuentra radicada en varios países de Latinoamérica, para el proyecto propuesto se seleccionó la sucursal de la ciudad de Bogotá capital de Colombia en la Carrera 19 # 114 – 65 Piso 4, en el Nuevo Edificio Empresarial.

Figura 2. Ubicación Grupo TX

Fuente: Google Maps

Actualmente en el área de sistemas y tecnología de la organización, acuerdo a visita técnica no se evidenció un Sistema de Gestión de Seguridad de la Información, por lo cual los riesgos en cuanto a incidentes de seguridad aumentan día a día, lo que podría conllevar a tener consecuencias tales como: la reducción en la productividad, pérdida de la reputación de la organización, perder oportunidad y competitividad en el mercado y posibles pérdidas financieras.

8. MARCO METODOLOGICO

8.1 UNIDAD DE ANALISIS

La unidad de análisis en la que se desarrollará el proyecto es la sede de Bogotá Colombia de Grupo TX, específicamente aplicada al área de sistemas y tecnología.

8.2 POBLACIÓN Y MUESTRA

8.2.1 Población. El proyecto está dirigido a todos los usuarios del área de sistemas y tecnología de Grupo TX en la sucursal de Bogotá Colombia, que de alguna manera participan en el proceso del área y pueden estar involucrados en un incidente informático.

8.2.2 Muestra. El proceso de soporte del área de sistemas y tecnología se toma como muestra, enfatizando el tratamiento de incidentes.

8.3 ETAPAS

Para el desarrollo, se identificaron 3 etapas, que se describen a continuación.

8.3.1 Etapa 1: Investigación y reconocimiento de información. En esta etapa, se realiza la recopilación de información, verificando los diferentes procesos y procedimientos del área de sistemas, entendiendo la dinámica del negocio y sus

particularidades, además de la valiosa información que los usuarios proporcionarán, además de esto, la referencia libros y los diferentes estándares en los que se basará el modelo.

8.3.2 Etapa 2: Definición de roles y aplicación del conocimiento. Detecta las diferentes vulnerabilidades a las que está expuesta el área de sistemas, la información de la empresa y el tratamiento que se tiene al momento de identificar un incidente, esto para su posterior análisis.

Se determinan los roles y responsabilidades de cada actor en la implementación del modelo.

Examinar las políticas y medidas de seguridad informática existentes, actualmente aplicadas en el área de sistemas de la compañía.

De acuerdo con los hallazgos realizados, determine la mejor solución de acuerdo con los requisitos comerciales para que el modelo propuesto sea acorde con ellos.

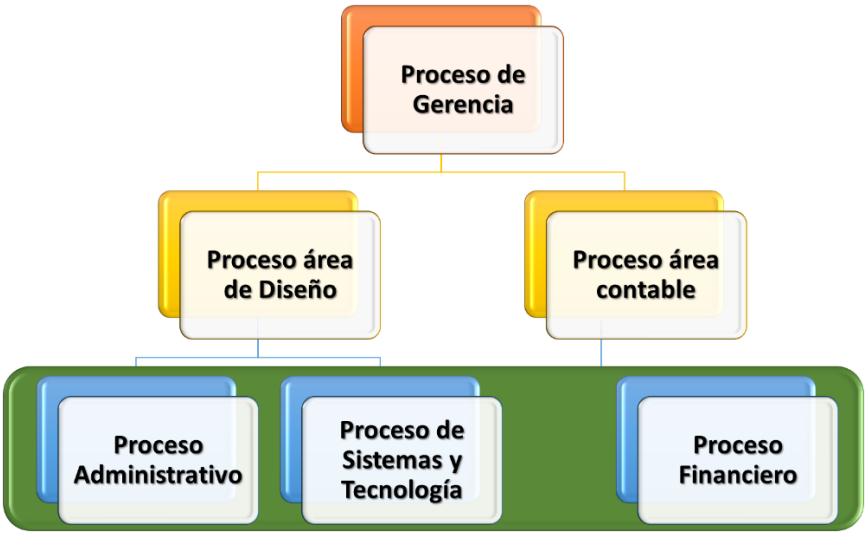
8.3.3 Etapa 3: Diseño. Se inicia con el diseño de políticas de seguridad, proceso de sistemas y tecnología, procedimiento de gestión de incidentes y toda la documentación correspondiente. Posteriormente, se analizan los resultados y se realizan correcciones.

9. VIABILIDAD

9.1 IDENTIFIACIÓN DE PROCESOS

De acuerdo a visita técnica realizada no se evidencia un sistema de gestión ni de calidad ni de seguridad informática, por lo tanto no se tiene un mapa de procesos, por eso se diseñó un mapa básico, como se puede ver en la figura 3, en el que se puede observar la composición operativa de la entidad, y por lo tanto ser capaz de comprender cómo el proceso de tecnología y sistemas, que se está evaluando, es un proceso de soporte que respalda los procesos misionales y es extremadamente importante para lograr el desarrollo y la continuidad del negocio, dentro de esta identificación, se evidencia que el proceso misional de diseño tiene un papel fundamental dentro de la compañía y que tiene características especiales y un tratamiento de la información y de los usuarios particulares, por lo tanto, esta información debe tenerse en cuenta a la hora de proponer las soluciones pertinentes, para que se adapten al proceso y no sean un obstáculo en el mapa de procesos de la organización.

Figura 3. Mapa de Procesos Grupo TX



Fuente: El Autor

9.2 RECURSOS

9.2.1 Información. La información, tanto interna como externa, es el activo más importante para la empresa, los objetivos del negocio dependen de ella, a esta información que se puede clasificar de acuerdo con el proceso al que pertenece, se debe garantizar un tratamiento especial para afianzar su seguridad. En la información que se analizó, se puede catalogar la información interna como la del área contable y administrativa, la información externa que pertenece a los clientes y para la cual generalmente se firman acuerdos de confidencialidad. La información junto con cada responsable se clasifica de la siguiente manera en la tabla 2:

Tabla 2. Inventario / Información

Información (Nombre)	Responsable	Descripción	Categoría	Ubicación
Información de Gestión contable	El Gerente General y/o Director de sistemas y tecnología	Bases de datos alimentadas por los aplicativos World Office Helissa, por medio de Microsoft SQL Server.	Datos Digitales	Servidor de aplicaciones y BD, DELL
Información de Gestión administrativa	El Gerente General y/o Director de sistemas y tecnología	Bases de datos alimentadas por el aplicativo WorldOffice por medio de Microsoft SQL Server.	Datos Digitales	Servidor de aplicaciones y BD, DELL
Información digital y confidencial de clientes	El Gerente General y/o Director de sistemas y tecnología	Material digital, de clientes para el desarrollo de servicios relacionados con mercadeo.	Datos Digitales	LACIE 2BIG NETWORK V 1.2 y arreglos de discos WD 3.0 tipo Nas. / DVD´s en archivo
Información digital general para los proyectos.	El Gerente General y/o Director de sistemas y tecnología	Material digital, de clientes para el desarrollo campañas de publicidad.	Datos Digitales	LACIE 2BIG NETWORK V 1.2 y arreglos de discos WD 3.0 tipo Nas. / DVD´s en archivo
Información de operación de cada usuario	El Gerente General y/o Director de sistemas y tecnología	Contenido digital, (Archivos Word, Excel, Power ponit, pst de Outlook, .pdf, etc...)	Datos Digitales	Portátiles, pc´s y equipos Mac, que se encuentran inventariados y pertenecen a la entidad.

Fuente: Autor

9.2.2 Recursos Humanos. Se destina tiempo de trabajo por parte del personal del área de tecnología y administrativa, que se traduce en horas hombre especializado. Las personas y áreas que participan para obtener la información necesaria, y realización de pruebas, son el área de sistemas y tecnología y administrativa, contando previamente con la autorización de la dirección de cada una.

9.2.3 Recursos físicos. Es importante tener la identificación de los recursos físicos del proceso, ya que son parte de las entradas para administrar la seguridad de la información.

9.2.3.1 Hardware. En la Tabla 3 se detallan los activos de hardware, que sirven como entradas para tener en cuenta en el inventario del proceso y así poder llevar a cabo controles y verificaciones sobre ellos.

Tabla 3. Inventario/ Hardware

Recurso Físico	Responsable	Categoría	Ubicación
4 Torres Mac Pro 2,8 Quad Core Intel Xeon 6GB Ram	El Gerente General y/o Director de sistemas y tecnología	Hardware	Oficina Bogotá / Área de Programación.
6 Portatiles DELL Vostro Intel Core I5 4Gb Ram	El Gerente General y/o Director de sistemas y tecnología	Hardware	Oficina Bogotá / Gerencia y Área administrativa contable y cuentas.
7 Computadores DELL Vostro Intel Core I5 4Gb Ram	El Gerente General y/o Director de sistemas y tecnología	Hardware	Oficina Bogotá / Área administrativa, contable y cuentas.
Portatil HP Intel Core I7 6 GB Ram	El Gerente General y/o Director de sistemas y tecnología	Hardware	Oficina Bogotá / Área de publicidad.

Fuente: Autor

Tabla 3. (continuación)

Recurso Físico	Responsable	Categoría	Ubicación
3 portátiles MacPro 4Gb Ram	El Gerente General y/o Director de sistemas y tecnología	Hardware	Oficina Bogotá/ Área de Programación
30 teléfonos IP	El Gerente General y/o Director de sistemas y tecnología	Hardware	Oficina Bogotá.
Sistema y Control de Alarmas y sensores	El Gerente General y/o Director de sistemas y tecnología	Hardware	Oficina Bogotá / Cuarto de informática / Rack
LACIE 2BIG NETWORK V 1.2 y arreglos de discos WD 3.0 tipo Nas.	El Gerente General y/o Director de sistemas y tecnología	Hardware	Oficina Bogotá / Cuarto de informática / Rack
2 impresoras fx1500	El Gerente General y/o Director de sistemas y tecnología	Hardware	Oficina Bogotá / Área Administrativa y contable
Red de datos, switches y red	El Gerente General y/o Director de sistemas y tecnología	Hardware	Oficina Bogotá
Servidor de dominio, DELL R270	El Gerente General y/o Director de sistemas y tecnología	Hardware	Oficina Bogotá / Cuarto de informática / Rack
Servidor de aplicaciones y BD, DELL	El Gerente General y/o Director de sistemas y tecnología	Hardware	Oficina Bogotá / Cuarto de informática / Rack
Servidor de servicios, DELL	El Gerente General y/o Director de sistemas y tecnología	Hardware	Oficina Bogotá / Cuarto de informática / Rack
Servidor de Telefonía IP Elastix 2.5	El Gerente General y/o Director de sistemas y tecnología	Hardware	Oficina Bogotá / Cuarto de informática / Rack
Firewall Watchguard Firebox T35	El Gerente General y/o Director de sistemas y tecnología	Hardware	Oficina Bogotá / Cuarto de informática / Rack

Fuente: Autor

9.2.3.2 Software y / o licencias. A pesar de ser recursos físicamente intangibles, las licencias que entrarán en el modelo se mencionarán en el documento porque la forma en que las usan los usuarios afecta directamente la implementación del modelo propuesto.

Además de esto, como ya se mencionó, se debe tener todo el software debidamente licenciado y actualizado. Algunas de las licencias se pueden observar en la tabla 4, a continuación:

Tabla 4. Inventario / Software y licencias

Software/ licencias	Responsable	Descripción	Categoría	Ubicación
Adobe CS5 y CS6	Gerente General y/o Director de sistemas y tecnología	Software para el desarrollo y gestión de piezas de diseño	Aplicación.	3 PortatilMacPro4Gb Ram / 4 Torres Mac Pro 2,8 Quad Core Intel Xeon 6GB Ram
Antivirus Kaspersky	Gerente General y/o Director de sistemas y tecnología	Software para detectar y eliminar virus informático.	Aplicación.	Todos los equipos tanto de usuarios como servidores.
World Office y Helissa	El Gerente General y/o Director de sistemas y tecnología	Software para la realización de gestión contable.	Aplicación.	7 Pc Vostro 230 Intel Core 2 Duo E7500 4Gb Ram / Servidor de aplicaciones.
Mac Os X (Mountain Lion, Lion, Snow Leopard)	El Gerente General y/o Director de sistemas y tecnología	Sistema operativo de Mac	Aplicación.	Torres Mac Pro 2,8 Quad Core Intel Xeon 6GB Ram
Microsoft Windows 7 como sistema operativo	El Gerente General y/o Director de sistemas y tecnología	Sistema operativo de Microsoft	Aplicación.	Todos los Equipos Pc.
Microsoft Office 2016 (Word, Excel, Outlook, Powerpoint	El Gerente General y/o Director de sistemas y tecnología	Herramienta ofimática de Microsoft para Pc´s.	Aplicación.	Equipos Pc.
Microsoft Office 2019 (Word, Excel, Outlook, Powerpoint)	El Gerente General y/o Director de sistemas y tecnología	Herramienta ofimática de Microsoft para Pc´s.	Aplicación.	Equipos Pc.
Microsoft Office 2019 Para Mac,	El Gerente General y/o Director de sistemas y tecnología	Herramienta ofimática de Microsoft para Mac	Aplicación.	Todos los Equipos Mac
Microsoft Windows Server 2012 r2	El Gerente General y/o Director de sistemas y tecnología	Sistema operativo de Microsoft	Aplicación.	Servidor de aplicaciones
Microsoft Windows Server 2008 r2	El Gerente General y/o Director de sistemas y tecnología	Sistema operativo de Microsoft	Aplicación.	Servidor de servicios.
Microsoft Sql server 2012	El Gerente General y/o Director de sistemas y tecnología	Motor de bases de datos	Aplicación.	Servidor de aplicaciones

Fuente: Autor

9.2.3.3 Instalaciones. El proyecto se desarrolla en la sede de Bogotá, Colombia, en la zona norte de la ciudad, la oficina cuenta con 430 metros cuadrados para su

operación, la seguridad es monitoreada 7x24 por un tercero que es adicional a la seguridad del edificio donde se ubica.

9.3 PRESUPUESTO

A continuación, en la tabla 5 se detalla el presupuesto estimado para desarrollar el presente proyecto.

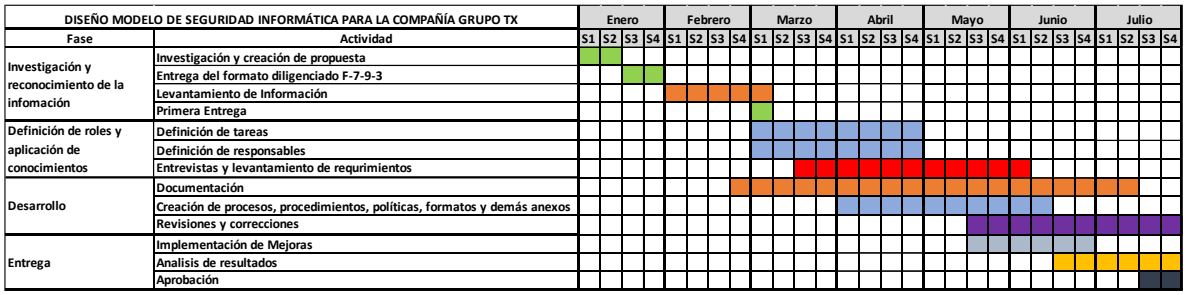
Tabla 5. Presupuesto

Descripción	Cantidad/Unidad	Valor Unitario	Valor Total
Equipo Humano (Hora ingeniero)	100	$ 150.000	$ 15.000.000
Equipos y Software	1	$ 1’799.000	$ 1’799.000
Viajes y Salidas de Campo	160	$ 2.500	$400.000
Materiales y Suministros	5	$ 50.000	$ 250.000
Total, Gastos			**$ 17.449.000**

Fuente: El Autor

9.4 CRONOGRAMA

Tabla 6. Cronograma



Fuente: El Autor

La tabla original del Cronograma se adjunta como anexo a este documento, para ser consultado en detalle.

10. CARATERIZACIÓN DEL PROCESO DE GESTIOÓN DE SISTEMAS Y TECNOLOGÍA Y PROCEDIMEINTO DE GESTIÓN DE INCIDENTES

Para desarrollar un esquema de seguridad de la información en el área de sistemas y tecnología de la organización, es esencial tener una caracterización del proceso involucrado, para así poder tener en detalle el procedimiento de gestión de incidentes en detalle y cumplir con el propósito de este proyecto.

10.1 PROCESO DE GESTIÓN DE SISTEMAS Y TECNOLOGÍA

El proceso original se encuentra como un documento anexo a este documento, en el diseño de la caracterización del proceso de sistemas y tecnología, los responsables del proceso están incluidos, iniciados por la alta gerencia y seguidos por el Director de Área, y el procedimiento que depende de este proceso y los insumos con los cuales se generan sus entradas y salidas.

La caracterización del proceso es extremadamente importante ya que es la guía del proceso y se heredan y describen:

- Procedimientos.
- Responsable.
- Indicadores de gestión.
- Suministros.
- Características del servicio.
- Objetivos.
- Alcance.
- Descripción de los clientes del proceso.
- Infraestructura.
- versión y normas.

A continuación, se puede ver el esquema en la tabla 7.

Tabla 7. Proceso de gestión de sistemas y tecnología

Grupo Tx	PROCESO DE GESTION DE SISTEMAS Y TECNOLOGIA	Código: SGSI-111 Versión: 01 Fecha: 20 de mayo de 2020 Página: 1 de 6

CAPITULO No. 1 PLANEACIÓN	
OBJETIVOS DE CALIDAD DEL PROCESO	Propender de la disponibilidad de la infraestructura tecnológica y la oportunidad en la atención de las diferentes solicitudes de la Compañía.
ALCANCE DEL PROCESO	Aplica a todo el personal de la compañía. Inicia con la recepción de la solicitud formal de la necesidad y/o requerimiento e incidentes y termina con la entrega y solución del requerimiento solicitado.
RESPONSABLE DEL PROCESO	Alta Gerencia y/o Director de sistemas

PROCESO DE INTERACCION					
PROVEEDORES (Interno y Externo)	**ENTRADA Y/O INSUMOS**	**PROCEDIMIENTOS Y/O ACTIVIDADES**	**SALIDAS Y/O PRODUCTOS**	**CARACTERISTICAS**	**CLIENTES (Internos y Externos)**
Todos los procesos de la compañía	Solicitud formal del requerimiento o identifiación de incidente (01-01-SGSI-03)	Procedimiento Gestión de incidentes	Reporte en la Planilla General de Asignación y Atención de Servicio	Oportunidad	Todos los procesos de la Compañía
Usuarios de la Compañía	Solicitud formal del requerimiento o identifiación de incidente (01-01-SGSI-03)	Procedimiento Gestión de incidentes	Reporte en la Planilla General de Asignación y Atención de Servicio	Disponibilidad Cumplimiento	Usuarios de la Compañía
Usuarios de la Compañía	Solicitud formal del requerimiento o identifiación de incidente (01-01-SGSI-03)	Procedimiento Gestión de incidentes	Planilla de Capacitación	Disponibilidad Cumplimiento	Usuarios de la Compañía

Fuente: Autor

Se crearon los indicadores de gestión del proceso, diseñados para medir el cumplimiento de procedimientos y verificar el cumplimiento. También están los registros y los criterios de aceptación. En la tabla 8 se puede apreciar, el documento original se encuentra anexo.

Tabla 8. Indicadores de Gestión-Resultados.

Grupo Tx	PROCESO DE GESTION DE SISTEMAS Y TECNOLOGIA	Código: SGSI-111 Versión: 01 Fecha: 20 de mayo de 2020 Página: 2 de 6

CAPITULO No. 2 RECURSOS		
RECURSO HUMANO (Cargos)	**INFRAESRUCTURA**	**AMBIENTE DE TRABAJO**
Gerente General	Equpos de Cómputo	Iluminación
Director de Sistemas	Puestos de Trabajo	Espacio
Ingenieros y Técnicos	Insumos de Oficina	Ventilación

CAPITULO No. 3 VERIFICACIÓN Y CONTROL (Indicadores de Control de Proceso)					
QUÉ SE CONTROLA?	**QUIEN?**	**CÓMO? - ACCIÓN**	**FRECUENCIA**	**REGISTRO ASOCIADO AL CONTROL**	**CRITERIO DE ACEPTACION**
Seguridad de la Información	Director de Sistemas y Tecnología y/o Director Administrativo	Monitoreo continuo a la infraestructura Tecnológica de la compañía	Por evento	Bitácora de novedades e incidentes (creada por el responsable del proceso)	Que lo solicitado sea coherente con lo entregado
Seguridad de la Información	Director de Sistemas y Tecnología y/o Director Administrativo	Plan de mejoramiento continuo mediante el ciclo Deming	Conforme al plan de trabajo	Bitácora de novedades e incidentes (creada por el responsable del proceso)	Que la información de la compañía cumpla con los principios básicos de la seguridad de la infomación (integridad, disponibilidad, confidencialidad)

CAPITULO No. 4 VERIFICACIÓN Y CONTROL (Indicadores de Control de Proceso - Resultado)				
OBJETIVO	**NOMBRE**	**META**	**INDICADOR (FORMULA)**	**RC: RESPONSABLE DEL CALCULO RAC: RESPONSABLE DEL ANALISIS Y SEGUMIENTO FD: FUENTE DE DATOS PC: PERIODICIDAD DEL CALCULO**
Garantizar la disponibilidad de la información	% de disponibilidad de la información	100% de disponibilidad de la información	(Horas de disponibilidad de la información / Total horas requeridas)*100	RC Y RAC: Directo de Sistemas FD: Bitácora de novedades e incidentes FC: Trimestral
Garantizar la disponibilidad de la información	% de disponibilidad de la información	100% de disponibilidad de la información	(Horas de integridad de la información / Total horas requeridas)*100	RC Y RAC: Directo de Sistemas FD: Bitácora de novedades e incidentes FC: Trimestral
Garantizar la disponibilidad de la información	% de disponibilidad de la información	100% de disponibilidad de la información	(Horas de confidencialidad de la información / Total horas requeridas)*100	RC Y RAC: Directo de Sistemas FD: Bitácora de novedades e incidentes

Fuente: Autor

Tabla 8 (Continuación)

Grupo Tx	PROCESO DE GESTION DE SISTEMAS Y TECNOLOGIA	Código: SGSI-111 Versión: 01 Fecha: 20 de mayo de 2020 Página: 3 de 6

CAPITULO No. 4 VERIFICACIÓN Y CONTROL (Indicadores de Control de Proceso - Resultado)				
OBJETIVO	**NOMBRE**	**META**	**INDICADOR (FORMULA)**	**RC: RESPONSABLE DEL CALCULO RAC: RESPONSABLE DEL ANALISIS Y SEGUMIENTO FD: FUENTE DE DATOS PC: PERIODICIDAD DEL CALCULO**
Satisfacer los requerimientos de los usuarios en cuanto a la seguridad de la información	Oportunidad en la Atención de requerimientos	100% de disponibilidad de la información	(Total de requerimientos atendidos oportunamente / Total de requerimientos solicitados)*100	RC Y RAC: Directo de Sistemas FD: Bitácora de novedades (perfiles y usuarios) FC: Cuatrimestre
Identificar el nivel de satisfacción de los usuarios (internos)	% de satisfacción en la prestación del servicio solicitado	Por definir, luego de la implementación	(No. De trabajadores satisfechos / Total de trabajadores encuestados)*100	RC Y RAC: Directo de Sistemas FD: Resultados de Encuesta FC: Anualmente

Grupo Tx	PROCESO DE GESTION DE SISTEMAS Y TECNOLOGIA	Código: SGSI-111 Versión: 01 Fecha: 20 de mayo de 2020 Página: 5 de 6

CAPITULO No. 5 DOCUMENTACIÓN ASOCIADA	
PROCEDIMIENTO Y / O INSTRUCTIVO Y / O REGISTROS	**CÓDIGO**
Procedimiento Gestión del Riego	01-01-SGSI

DOCUMENTOS DE REFERENCIA	**ORIGEN**		
DESCRIPCION	**INTERNACIONAL**	**NACIONAL**	**INTERNO**
Norma Técnica Internacional 9001:2008 / Norma Internacional 27001:	**X**		

Grupo Tx	PROCESO DE GESTION DE SISTEMAS Y TECNOLOGIA	Código: SGSI-111 Versión: 01 Fecha: 20 de mayo de 2020 Página: 6 de 6

CAPITULO No. 6 CONTROL DE CAMBIOS		
VERSIÓN	**FECHA VIGENCIA**	**DESCRIPCION DE CAMBIOS**
01		N/A

Fuente: Autor

10.2 PROCEDIMIENTO DE GESTIÓN DE INCIDENTES

Se diseñó el procedimiento de gestión de incidentes, que describe el tratamiento que se le da al identificar un incidente o recibir una solicitud; Contiene los responsables, formatos y registros correspondientes a cada caso, se adjunta el documento completo se encuentra anexo, y fue diseñado teniendo en cuenta las características del negocio y las directrices de la alta gerencia.

10.2.1 Objetivo del procedimiento. Realizar gestión de incidentes del área de sistemas y tecnología, para garantizar la integridad, disponibilidad y confidencialidad de la información.

10.2.2 Alcance del procedimiento. Se aplica a todo el personal de Grupo TX, comienza con la necesidad de salvaguardar y garantizar los principios de seguridad informática sobre un requerimiento o incidente identificado y termina con la custodia y / o satisfacción de los requerimientos que tienen que ver con la información de la compañía.

10.2.3 Responsabilidades. El Gerente General y / o Director de Sistemas y Tecnología, así como los colaboradores designados responden por el funcionamiento de la Infraestructura Tecnología de la Compañía.

10.2.3 Generalidades. La información a la que se hace referencia en este documento es la producida o modificada en los procesos de Grupo TX, que se ha generado utilizando los recursos de la misma o de acuerdo con las funciones o responsabilidades de los colaboradores; el objetivo es definir las condiciones y términos para disponer de la información de propiedad de la compañía a clientes externos e internos del proceso. La entrega de la información a otras entidades y personas naturales, solo se puede hacer si existe una solicitud formal y previamente aprobada por el Gerente General y / o el Director de Sistemas y Tecnología. Está totalmente prohibido entregar información de manera informal en respuesta a solicitudes verbales, siempre debe existir un soporte físico.

El uso que las entidades externas le dan a la información de Grupo TX está sujeto a los derechos de propiedad que la compañía tiene sobre ella.

10.2.5 Registros. Se diseñaron varios registros que se aplican de acuerdo con el desarrollo del procedimiento, en la tabla 9 los registros están relacionados.

Tabla 9. Registros

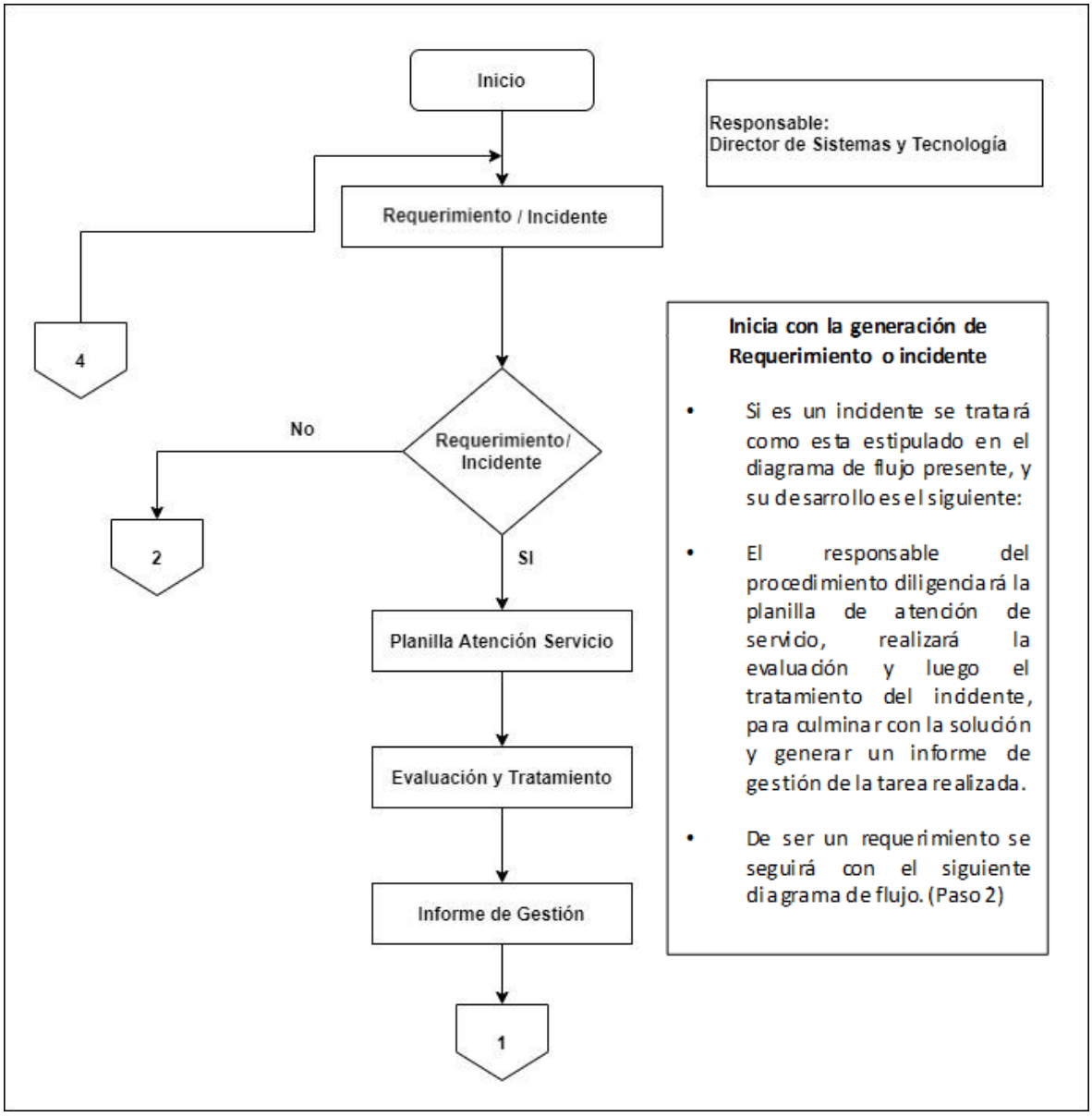
Clase	Título Del Documento	Código	Disposición
Formato	Solicitud formal del requerimiento /Incidente	01-01-SGSI-03	Se conserva en medio físico y magnético
Formato	Planilla General de Asignación y Atención de Servicio	01-01- SGSI - 04	Se conserva en medio físico y magnético
Formato	Plan de Capacitación	01-01- SGSI - 05	Se conserva en medio físico y magnético
Formato	Planilla de Back Up	01-01- SGSI - 06	Se conserva en medio físico y magnético
Registro	Informe de Prestación de Gestión	N.A.	Se conserva en medio físico y magnético

Fuente: Autor

10.2.6 Desarrollo. A continuación, en la figura 4, puede ver el diagrama de flujo que describe el desarrollo del procedimiento, que se divide en 3 fases, debe tenerse en cuenta que dentro del procedimiento está la solicitud de realizar una copia de seguridad como requerimiento por parte de los usuarios del proceso y también con un cronograma establecido que debe completarse con la planilla de Backup[16].

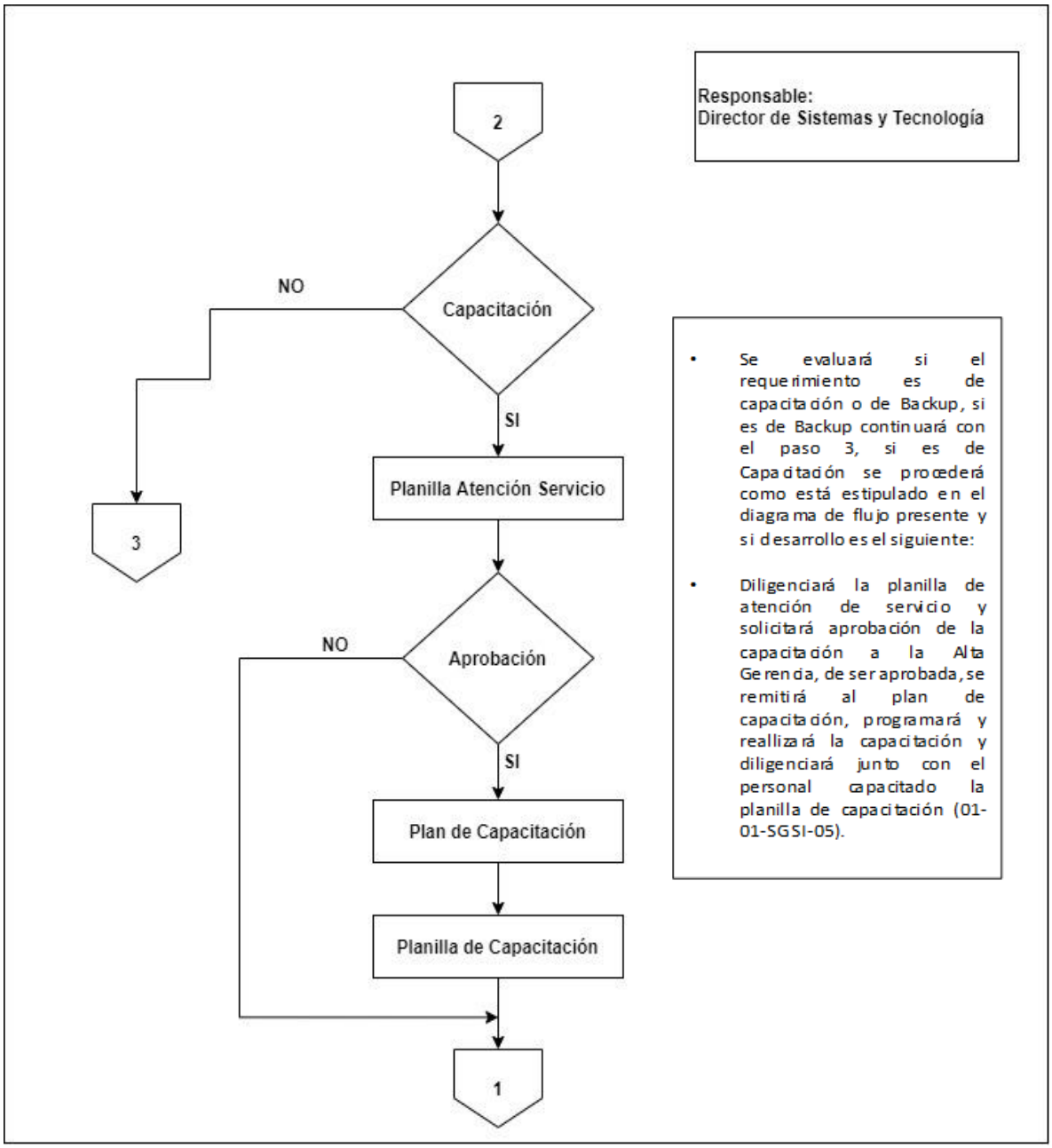
[16] Ibarra Quevedo, Raúl Serrano López, Miguel Angel Calixto Garera y González, Carlos. Teoría de la información y encriptamiento de datos. Instituto Politécnico Nacional. Ed 1, 2010, pág 168

Figura 4. Fase 1 Procedimiento gestión de incidentes.



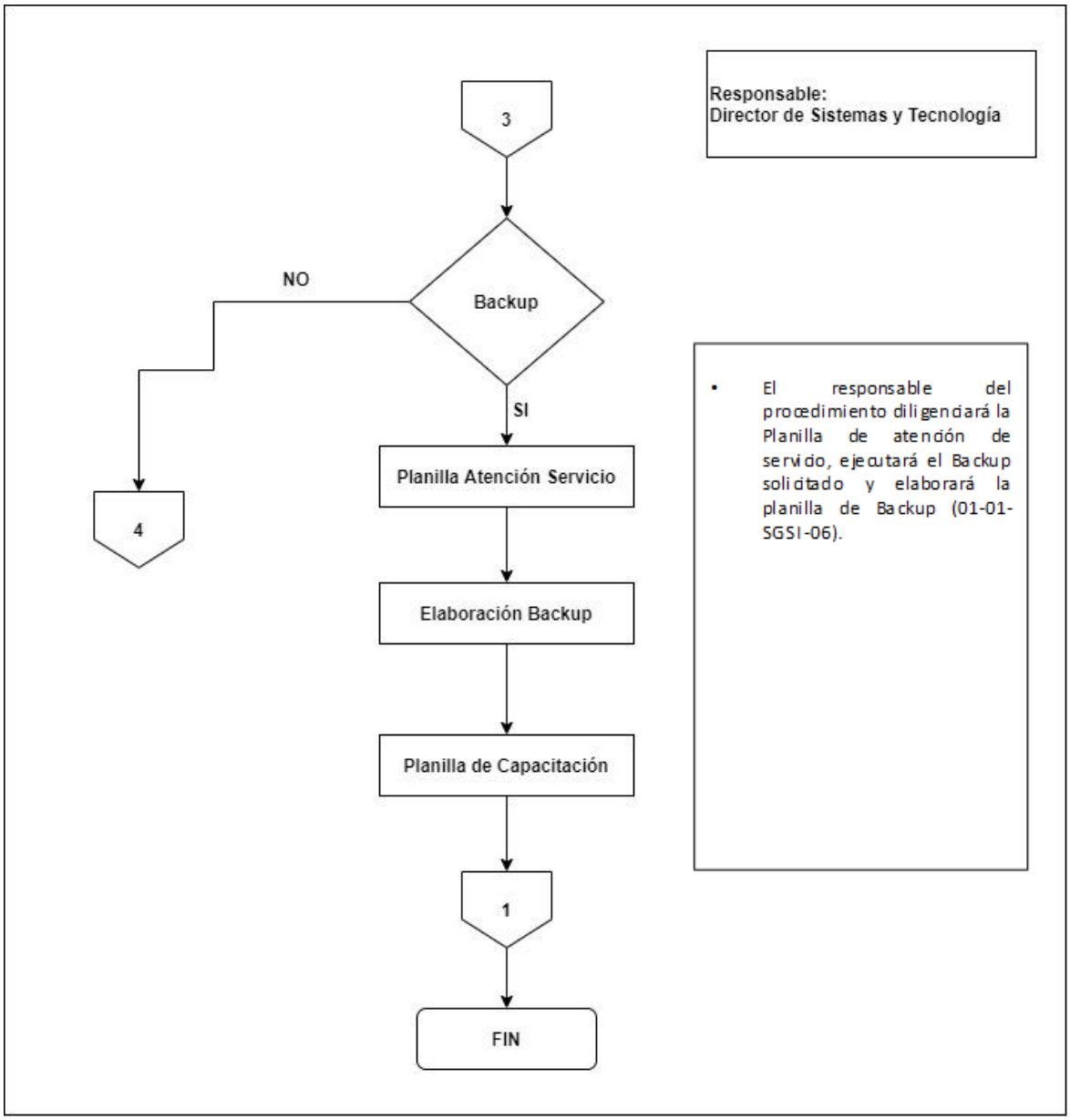
Fuente: Autor

Figura 5. Fase 2 Procedimiento gestión de incidentes.



Fuente: Autor

Figura 6. Fase 3 Procedimiento Gestión de Incidentes.



Fuente: Autor

11. ENCUESTA INTERNA SOBRE EL RESULTADO DE LA SEGURIDAD DE LA INFORMACIÓN ACTUAL EN GRUPO TX

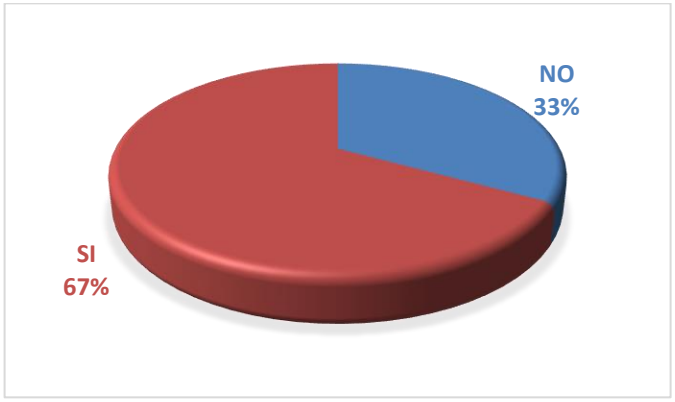
Para poder evidenciar las vulnerabilidades a las que el proceso de sistemas y tecnología se encuentra expuesto, es necesario realizar un diagnóstico para así poder tratar los riesgos y tomar las decisiones pertinentes, para ello se realizó una encuesta, basada en el formato de auto diagnóstico según los 133 controles que aplican de la norma ISO 27001, el cual se anexa para ser consultado en detalle, así se obtuvieron los siguientes resultados:

(Si, significa que cumple y no, si está en un porcentaje alto, que está por fuera del rango aceptable).

11.1 RESULTADOS AUTODIAGNÓSTICO

En general, en el resultado de la evaluación de autodiagnóstico, se puede ver cómo el 33% muestra riesgos que deben tenerse en cuenta. Para comenzar a tratar, en la figura 7, este resultado se ve gráficamente:

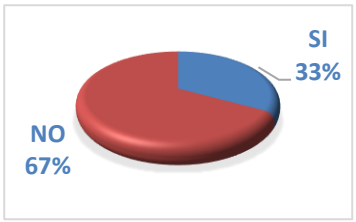
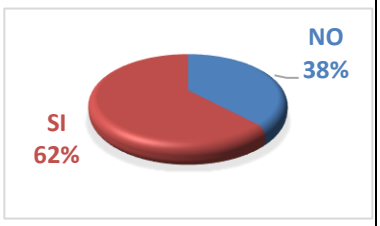
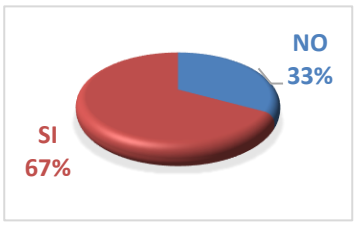
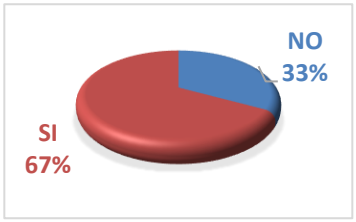
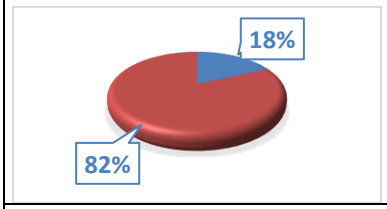
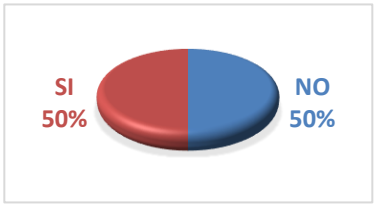
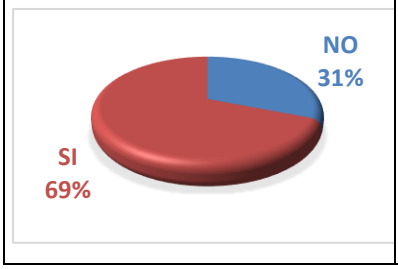
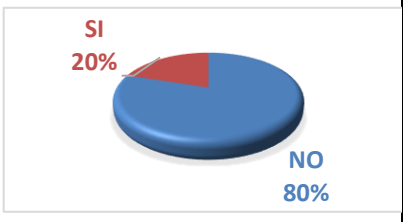
Figura 7. Auto diagnóstico General



Fuente: Autodiagnóstico ISO 27001

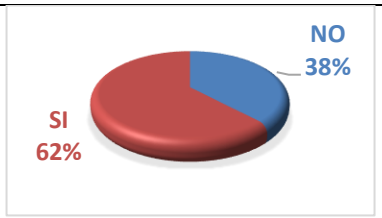
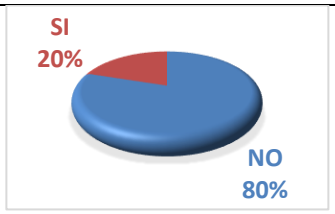
A continuación, en la tabla 10 se puede ver en detalle el resultado y según la clasificación de los controles, determinar cuáles serán los factores más críticos para tratar, dependiendo del nivel de aceptación de cada factor.

Tabla 10. Auto diagnóstico detallado

Políticas de seguridad	
	**Nivel aceptación de 33%**
Organización de la seguridad	
	**Nivel aceptación de 62%**
Clasificación y control de activos	
	**Nivel aceptación de 67%**
Seguridad del personal	
	**Nivel aceptación de 33%**
Seguridad física y del entorno	
	**Nivel aceptación de 82%**
Gestión de comunicaciones y operaciones	
	**Nivel aceptación de 50%**
Control de accesos	
	**Nivel aceptación de 69%**
Gestión de continuidad del negocio	
	**Nivel aceptación de 20%**

Fuente: Autodiagnóstico ISO 27001

Tabla 10. (Continuación)

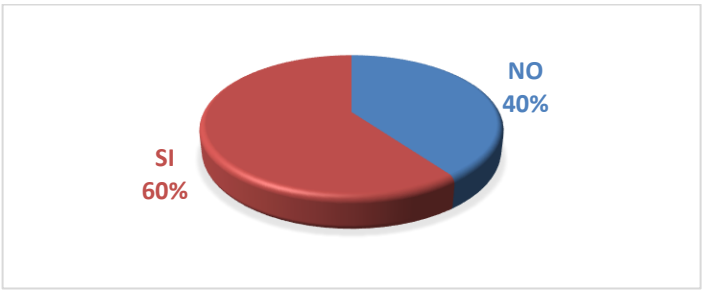
Desarrollo y mantenimiento de sistemas		Administración de incidentes	
	Nivel aceptación de 62%		Nivel aceptación de 20%

Fuente: Autodiagnóstico ISO 27001

Los resultados obtenidos en las anteriores gráficas de la Tabla 10, pueden ser observarse en la clasificación de los controles, que se encuentran en el anexo A.

A continuación, en la figura 8 de conformidad total, se muestra el panorama general de la compañía, con respecto a los controles verificados.

Figura 8. Conformidad Total



Fuente: Autodiagnóstico ISO 27001

Con estos resultados, se puede evidenciar la importancia del modelo logrado en este proyecto, ya que, si bien se obtiene un nivel general aceptable de cumplimiento, el manejo de incidentes y la continuidad del negocio se encuentra en niveles poco aceptables y no satisface los requerimientos del negocio ni de la alta gerencia. También es evidente que la compañía no tiene usuarios bien capacitados en la identificación de incidentes, y esto hace que los tiempos de respuesta del área de Sistemas y Tecnología sean aún más retrasados, ya que

pierden mucho tiempo validando y clasificando incidentes, además no se documentan las soluciones dadas a los usuarios.

El ejercicio permite exponer a la gerencia la importancia del tratamiento de incidentes y hace que demás procesos sean conscientes de los riesgos generados por un mal manejo de los incidentes dentro de la organización.

12. RESULTADOS

Al finalizar el proyecto se esperan obtener los siguientes resultados.

- Mejorar la gestión y custodia de la información en el área de sistemas y tecnología de Grupo TX.

- Promover, familiarizar y sensibilizar a todos los usuarios de procesos en el área de sistemas y tecnología, con la importancia de mantener buenas prácticas con el uso de la información.

- Este documento se presentará como un informe de gestión con el análisis resultante del diseño del modelo de seguridad.

- Optimizar el tratamiento dado a los incidentes para mitigar los riesgos que puedan afectar el negocio y su continuidad.

- Mejorar en la operación de la infraestructura del sistema, gracias a la documentación de incidentes.

- Lograr la independencia en la resolución de incidentes con respecto a futuros cambios con los responsables, gracias a la documentación.

- Optimizar los tiempos de respuesta a incidentes presentados en el área de sistemas y tecnología.

- Instituir cultura de identificación y prevención de incidentes dentro de la entidad.

CONCLUSIONES

- Es necesario monitorear periódicamente el tratamiento que se le den a los incidentes que se identifiquen, porque es un negocio cambiante y los requisitos del cliente también cambian.

- Este documento puede tomarse como referencia para mostrar que, independientemente de las particularidades de un negocio, si se pueden aplicar controles de seguridad sin afectar la continuidad del negocio y su esencia.

- Es importante involucrar a todas las áreas y usuarios que de alguna manera afectan la seguridad de la información, porque los incidentes pueden ocurrir desde cualquier frente, para ello es esencial capacitar a todos los funcionarios que intervienen en el tratamiento de la información, ya que a partir de sus buenas prácticas y competencias se puede construir un buen modelo de gestión de seguridad de la información.

- Con la documentación generada en el histórico de incidencias, pueden generarse buenas prácticas para prevenir futuras incidencias y así disminuir posibles riesgos, así como también poder mejorar los tiempos de respuesta a las incidencias.

RECOMENDACIONES

- Adicionalmente a las medidas propuestas en el modelo de sistema de gestión de seguridad, es de gran importancia adicionar un plan de contingencia para los servidores, ya que actualmente no existe un sistema de alta disponibilidad para los sistemas de información y bases de datos.

- Elaborar reuniones periódicas, con los involucrados en el proceso, para medir y retroalimentar la experiencia y mejorarla, así como también capacitarlos de acuerdo con el plan propuesto sobre buenas prácticas y haciendo hincapié en las competencias mínimas en TIC que los usuarios deben tener.

- Planificar el diseño de otros procesos y procedimientos y no descartar la opción de trabajar para lograr la certificación en calidad y / o seguridad de la información.

- La forma de referirse al área de tecnología y sistemas podría ajustarse a las tecnologías de la información y la comunicación (TIC) para que sea más conveniente para los servicios que brinda y de acuerdo con su misión, aunque es un cambio más que sustancial ayudaría a mejorar la percepción del área por parte de todos los funcionarios.

- Es importante que, en el momento de la apropiación de la solución, todas las áreas estén activas y a favor del sistema, guiadas por la alta gerencia.

BIBLIOGRAFÍA

ERB, Markus. Gestión de riesgo en la seguridad informática: Facilitando el manejo seguro de la información en organizaciones sociales [en línea]. [Consultado el día 08 de enero de 2020]. Disponible en http://protejete.wordpress.com

FARAONI, Luis. ernst & young revela escasa importancia otorgada a la seguridad informática: Noticias Financieras. [En línea]. Editorial Global Network Content Services LLC, DBA Noticias Financieras LLC. [Consultado el día 9 de Enero de 2020 en ProQuest]. Disponible en http://ezproxy.unbosque.edu.co:2080/docview/466101556?accountid=41311

INSTITUTO COLOMBIANODE NORMAS TÉCNICAS Y CERTIFICACIÓN. Trabajos escritos: presentación de tesis, trabajos de grado y otros trabajos de investigación. 6 ed. Bogotá D.C: INCONTEC, 2008 (NTC 1486)

LÓPEZ NEIRA, Agustín y RUIZ SPOHR, Javier.El portal de ISO 27001 en español, ISO 27000. [Citado 11 de Enero de 2020], disponible en: http://www.iso27000.es/index.html

Ibarra Quevedo, Raúl Serrano López, Miguel Angel Calixto Garera y González, Carlos. Teoría de la información y encriptamiento de datos. Instituto Politécnico

Nacional. Ed 1, 2010, pág 11

HERNÁNDEZ SAMPIERI, C. Roberto; FERNÁNDEZ COLLADO, Carlos y BAPTISTA, pilar. Metodología de la investigación, Bogotá D.C: Editorial Mcgraw-Hill. Panamericana, 1997

GÓMEZ VIEITES, Álvaro. Enciclopedia de la seguridad informática, 2 ed. México: Alfaomega, 2011.

IBARRA QUEVEDO, Raul. SERRANO LÓPEZ, Miguel Angel Calixto Garera y GONZALEZ, Carlos. Teoría de la información y encriptamiento de datos, México: Instituto Politécnico Nacional. 2010

PEACH, Robert W. Manual de ISO 9000 ed. 3, McGraw-Hill Interamericana, 1999, pág. 37-59.

SINGH SOIN, Sarv. Control de calidad total: claves, metodologías y administración para el éxito, McGraw-Hill Interamericana, 2011, pág.94-96

NIÑO ROJAS, Víctor miguel. Metodología de la Investigación: diseño y ejecución, Colombia: Ediciones de la U, 2011.

LÓPEZ MATACHANA, Yansenis, Los virus informáticos: una amenaza para la sociedad, Cuba: Editorial Universitaria, 2009.

ANEXO A

AUTODIAGNOSTICO ISO 27001 GRUPO TX

Tabla A1. Auto diagnóstico General Grupo TX

FORMULARIO PARA AUTODIAGNÓSTICO GRUPO TX	Grupo Tx			
POLITICAS DE SEGURIDAD				
- Existen documento(S) de políticas de seguridad de SI	☐ FALSO	0		
- Existe normativa relativa a la seguridad de los SI	☑ VERDADERO	1		
- Existen procedimientos relativos a la seguridad de SI	☐ FALSO	0		
- Existe un responsable de las políticas, normas y procedimientos	☑ VERDADERO	1		
- Existen mecanismos para la comunicación a los usuarios de las normas	☐ FALSO	0		
- Existen controles regulares para verificar la efectividad de las políticas	☐ FALSO	0	**SI**	**NO**
		2	**33,33**	**66,67**
ORGANIZACIÓN DE LA SEGURIDAD				
- Existen roles y responsabilidades definidos para las personas implicadas en la seguridad	☑ VERDADERO	1		
- Existe un responsable encargado de evaluar la adquisición y cambios de SI	☑ VERDADERO	1		
- La dirección y las áreas de la organización participan en temas de seguridad	☐ FALSO	0		
- Existen condiciones contractuales de seguridad con terceros y outsoursing	☑ VERDADERO	1		
- Existen criterios de seguridad en el manejo de terceras partes	☑ VERDADERO	1		
- Existen programas de formación en seguridad para los colaboradores, clientes y terceros	☐ FALSO	0		
- Existe un acuerdo de confidencialidad de la información que se accesa	☑ VERDADERO	1		
- Se revisa la organización de la seguridad periódicamente por una empresa externa	☑ FALSO	0	**SI**	**NO**
		5	**62,50**	**37,50**
ADMINISTRACIÓN DE ACTIVOS				
-Existe un inventario de activos actualizado	☑ VERDADERO	1		
-El inventario contiene activos de datos, software, equipos y servicios	☑ VERDADERO	1		
-Se dispone de una clasificación de la información según la criticidad de la misma	☐ FALSO	0		
-Existe un responsable de los activos	☑ VERDADERO	1		
-Existen procedimientos para clasificar la información	☐ FALSO	0		
-Existen procedimientos de etiquetado de la información	☑ VERDADERO	1	**SI**	**NO**
		4	**66,67**	**33,33**
SEGURIDAD DE LOS RRHH				
-Se tienen definidas las responsabilidades y roles de seguridad	☑ VERDADERO	1		
- Se tiene en cuenta la seguridad en la selección y baja del personal	☑ VERDADERO	1		
- Se plasman las condiciones de confidencialidad y responsabilidades en los contratos	☑ VERDADERO	1		
- Se imparte la formación adecuada de seguridad y tratamiento de activos	☐ FALSO	0		
- Existe un canal y procedimientos claros a seguir en caso de incidentes de seguridad	☐ FALSO	0		
- Se recogen los datos de los incidentes de forma detallada	☐ FALSO	0		
- Informan los usuarios de las vulnerabilidades observadas o sospechadas	☐ FALSO	0		
- Se informa a los usuarios de que no deben, bajo ninguna circunstancia probar las vulnerabilidades	☐ FALSO	0		
- Existe un proceso disciplinario de la seguridad de la información	☐ FALSO	0	**SI**	**NO**
		3	**33,33**	**66,67**
SEGURIDAD FÍSICA Y DEL AMBIENTE				
- Existe perímetro de seguridad física (una pared, puerta con llave)	☑ VERDADERO	1		
- Existen controles de entrada para protegerse frente al acceso de personal no autorizado	☑ VERDADERO	1		
- Un área segura ha de estar cerrada, aislada y protegida de eventos naturales	☑ VERDADERO	1		
- En las áreas de carga y expedición están aisladas de las áreas de SI	☑ VERDADERO	1		
- La ubicación de los equipos está del tal manera para minimizar accesos innecesarios	☑ VERDADERO	1		
- Existen protecciones frente a fallas de la alimentación eléctrica	☑ VERDADERO	1		
- Existe seguridad en el cableado frente a daños e intercepciones	☑ VERDADERO	1		
- Se asegura la disponibilidad e integridad de todos los equipos	☑ VERDADERO	1		
- Existe algún tipo de seguridad para los equipos retirados o ubicados exteriormente	☐ FALSO	0		
- Se incluye la seguridad en los dispositivos móviles	☐ FALSO	0		
		9	**81,82**	**18,18**

GESTIÓN DE COMUNICACIONES Y OPERACIONES				
- Todos los procedimientos operativos identificados en la política de seguridad han de estar documentados	☐ FALSO	0		
- Están establecidas las responsabilidades para controlar los cambios de equipos	☑ VERDADERO	1		
- Están establecidas las responsabilidades para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad	☐ FALSO	0		
- Existe algún método para reducir el mal uso accidental o deliberado de los sistemas	☐ FALSO	0		
- Existe una separación de los entornos de desarrollo y producción	☑ VERDADERO	1		
- Existen contratistas externos para la gestión de los Sistemas de Información	☑ VERDADERO	1		
- Existe un Plan de capacacidad para asegurar la adecuada capacidad de proceso y de almacenamiento	☐ FALSO	0		
- Existen criterios de aceptación de nuevos SI, incluyendo actualizaciones y nuevas versiones	☐ FALSO	0		
- Controles contra Software malicioso	☑ VERDADERO	1		
- Realizar copias de seguridad de la información esencial para el negocio	☑ VERDADERO	1		
- Existen logs para las actividades realizadas por los operadores y administradores	☑ VERDADERO	1		
- Existen logs de los fallos detectados	☐ FALSO	0		
- Existen rastros de auditoría	☐ FALSO	0		
- Existe algún control en las redes	☐ FALSO	0		
- Hay controles establecidos para realizar la gestión de los medios informáticos (cintas, discos removibles, informes impresos)	☑ VERDADERO	1		
- Eliminación de los medios informáticos. Pueden disponer de información sensible	☐ FALSO	0		
- Existe seguridad de la documentación de los sistemas	☐ FALSO	0		
- Existen acuerdos para intercambio de información y software	☑ VERDADERO	1		
- Existen medidas de seguridad de los medios en el tránsito	☐ FALSO	0		
- Existen medidas de seguridad en el comercio electrónico	☐ FALSO	0		
- Se han establecido e implantado medidas para proteger la confidencialidad e integridad de información publicada	☑ VERDADERO	1		
- Existen medidas de seguridad en las transacciones en línea	☑ VERDADERO	1		
- Se monitorean las actividades relacionadas a la seguridad	☐ FALSO	0	**SI**	**NO**
		10	**50,00**	**50,00**
CONTROL DE ACCESOS				
- Existe una política de control de accesos	☑ VERDADERO	1		
- Existe un procedimiento formal de registro y baja de accesos	☑ VERDADERO	1		
- Se controla y restringe la asignación y uso de privilegios en entornos multi-usuario	☑ VERDADERO	1		
- Existe una gestión de los password de los usuarios	☑ VERDADERO	1		
- Existe una revisión de los derechos de acceso de los usuarios	☐ FALSO	0		
- Existe el uso de los passwords	☑ VERDADERO	1		
- Se protege el acceso de los equipos desatendidos	☑ VERDADERO	1		
- Existen políticas de limpieza en el puesto de trabajo	☐ FALSO	0		
- Existe una política de uso de los servicios de red	☑ VERDADERO	1		
- Se asegura la ruta (path) desde el terminal al servicio	☐ FALSO	0		
- Existe una autenticación de usuarios en conexiones externas	☑ VERDADERO	1		
- Existe una autenticación de los nodos	☑ VERDADERO	1		
- Existe un control de la conexión de redes	☑ VERDADERO	1		
- Existe un control de routing de las redes	☐ FALSO	0		
- Existe una identificación única de usuario y una automática de terminales	☑ VERDADERO	1		
- Existen procedimientos de log-on al terminal	☐ FALSO	0		
- Se ha incorporado medidas de seguridad a la computación móvil	☐ FALSO	0		
- Está controlado el teletrabajo por la organización	☐ FALSO	0	**SI**	**NO**
		11	**68,75**	**31,25**
DESARROLLO Y MANTINIMIENTO DE LOS SISTEMAS				
- Se asegura que la seguridad está implantada en los sistemas de información	☐ FALSO	0		
- Existe seguridad en las aplicaciones	☑ VERDADERO	1		
- Existen controles criptográficos	☐ FALSO	0		
- Existe seguridad en los ficheros de los sistemas	☑ VERDADERO	1		
- Existe seguridad en los procesos de desarrollo, testing y soporte	☑ VERDADERO	1		
- Existen controles de seguridad para los resultados de los sitemas	☑ VERDADERO	1		
- Existe la gestión de los cambios en los SO	☑ VERDADERO	1		
- Se controlan las vulnerabilidades de los equipos	☐ FALSO	0	**SI**	**NO**
		5	**62,50**	**37,50**
ADMINISTRACION DE INCIDENTES				
- Se comunican los eventos de seguridad	☑ VERDADERO	1		
- Se comunican las debilidades de seguridad	☐ FALSO	0		
- Se encuentran definidas las responsabilidades antes de un incidente	☐ FALSO	0		
- Existe un procedimiento formal de respuesta	☐ FALSO	0		
- Existe la gestión de incidentes	☑ FALSO	0	**SI**	**NO**
		1	**20,00**	**80,00**

GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO				
- Existen procesos para la gestión de la continuidad	☑ VERDADERO	1		
- Existe un plan de continuidad del negocio y análisis de impacto	☐ FALSO	0		
- Existe un diseño, redacción e implementación de planes de continuidad	☐ FALSO	0		
- Existe un marco de planificación para la continuidad del negocio	☐ FALSO	0		
- Existen prueba, mantenimiento y reevaluación de los planes de continuidad del negocio	☐ FALSO	0	**SI**	**NO**
		1	**20,00**	**80,00**
CUMPLIMIENTO				
- Se tiene en cuenta el cumplimiento con la legislación por parte de los sistemas	☑ VERDADERO	1		
- Existe el resguardo de propiedad intelectual	☑ VERDADERO	1		
- Existe el resguardo de los registros de la organización	☑ VERDADERO	1		
- Existe una revisión de la política de seguridad y de la conformidad técnica	☐ FALSO	0		
- Existen consideraciones sobre las auditorias de los sistemas	☐ FALSO	0		
		3	**60,00**	**40,00**

Fuente: El Autor

ANEXO B

CARACTERIZACIÓN PROCESO GRUPO TX

Tabla B1. Caracterización proceso Grupo TX

Grupo Tx	PROCESO DE GESTIÓN DE SISTEMAS Y TECNOLOGÍA	Código: SGSI-111 Versión: 01 Fecha: 20 de mayo de 2020 Página: 1 de 6

CAPÍTULO No. 1 PLANEACIÓN	
OBJETIVOS DE CALIDAD DEL PROCESO	Propender de la disponibilidad de la infraestructura tecnológica y la oportunidad en la atención de las diferentes solicitudes de la Compañía.
ALCANCE DEL PROCESO	Aplica a todo el personal de la compañía. Inicia con la recepción de la solicitud formal de la necesidad y/o requerimiento e incidentes y termina con la entrega y solución del requerimiento solicitado.
RESPONSABLE DEL PROCESO	Alta Gerencia y/o Director de sistemas

PROCESO DE INTERACCIÓN					
PROVEEDORES (Interno y Externo)	**ENTRADA Y/O INSUMOS**	**PROCEDIMIENTOS Y/O ACTIVIDADES**	**SALIDAS Y/O PRODUCTOS**	**CARACTERÍSTICAS**	**CLIENTES (Internos y Externos)**
Todos los procesos de la compañía	Solicitud formal del requerimiento o identifiación de incidente (01-01-SGSI-03)	Procedimiento Gestión de incidentes	Reporte en la Planilla General de Asignación y Atención de Servicio	Oportunidad	Todos los procesos de la Compañía
Usuarios de la Compañía	Solicitud formal del requerimiento o identifiación de incidente (01-01-SGSI-03)	Procedimiento Gestión de incidentes	Reporte en la Planilla General de Asignación y Atención de Servicio	Disponibilidad Cumplimiento	Usuarios de la Compañía
Usuarios de la Compañía	Solicitud formal del requerimiento o identifiación de incidente (01-01-SGSI-03)	Procedimiento Gestión de incidentes	Planilla de Capacitación	Disponibilidad Cumplimiento	Usuarios de la Compañía

CAPÍTULO No. 2 RECURSOS		
RECURSO HUMANO (Cargos)	**INFRAESRUCTURA**	**AMBIENTE DE TRABAJO**
Gerente General	Equpos de Cómputo	Iluminación
Director de Sistemas	Puestos de Trabajo	Espacio
Ingenieros y Técnicos	Insumos de Oficina	Ventilación

CAPÍTULO No. 3 VERIFICACIÓN Y CONTROL (Indicadores de Control de Proceso)					
QUÉ SE CONTROLA?	**QUIÉN?**	**CÓMO? - ACCIÓN**	**FRECUENCIA**	**REGISTRO ASOCIADO AL CONTROL**	**CRITERIO DE ACEPTACIÓN**
Seguridad de la Información	Director de Sistemas y Tecnología y/o Director Administrativo	Monitoreo continuo a la infraestructura Tecnológica de la compañía	Por evento	Bitácora de novedades e incidentes (creada por el responsable del proceso)	Que lo solicitado sea coherente con lo entregado
Seguridad de la Información	Director de Sistemas y Tecnología y/o Director Administrativo	Plan de mejoramiento continuo mediante el ciclo Deming	Conforme al plan de trabajo	Bitácora de novedades e incidentes (creada por el responsable del proceso)	Que la información de la compañía cumpla con los principios básicos de la seguridad de la infomación (integridad, disponibilidad, confidencialidad)

CAPÍTULO No. 4 VERIFICACIÓN Y CONTROL (Indicadores de Control de Proceso - Resultado)				
OBJETIVO	**NOMBRE**	**META**	**INDICADOR (FORMULA)**	**RC: RESPONSABLE DEL CALCULO RAC: RESPONSABLE DEL ANALISIS Y SEGUMIENTO FD: FUENTE DE DATOS PC: PERIODICIDAD DEL CALCULO**
Garantizar la disponibilidad de la información	% de disponibilidad de la información	100% de disponibilidad de la información	(Horas de disponibilidad de la información / Total horas requeridas)*100	RC Y RAC: Directo de Sistemas FD: Bitácora de novedades e incidentes FC: Trimestral
Garantizar la disponibilidad de la información	% de disponibilidad de la información	100% de disponibilidad de la información	(Horas de integridad de la información / Total horas requeridas)*100	RC Y RAC: Directo de Sistemas FD: Bitácora de novedades e incidentes FC: Trimestral
Garantizar la disponibilidad de la información	% de disponibilidad de la información	100% de disponibilidad de la información	(Horas de confidencialidad de la información / Total horas requeridas)*100	RC Y RAC: Directo de Sistemas FD: Bitácora de novedades e incidentes
Satisfacer los requerimientos de los usuarios en cuanto a la seguridad de la información	Oportunidad en la Atención de requerimientos	100% de disponibilidad de la información	(Total de requerimientos atendidos oportunamente / Total de requerimientos solicitados)*100	RC Y RAC: Directo de Sistemas FD: Bitácora de novedades (perfiles y usuarios) FC: Cuatrimestre
Identificar el nivel de satisfacción de los usuarios (internos)	% de satisfacción en la prestación del servicio solicitado	Por definir, luego de la implementación	(No. De trabajadores satisfechos / Total de trabajadores encuestados)*100	RC Y RAC: Directo de Sistemas FD: Resultados de Encuesta FC: Anualmente

CAPITULO No. 5 DOCUMENTACIÓN ASOCIADA	
PROCEDIMIENTO Y / O INSTRUCTIVO Y / O REGISTROS	**CÓDIGO**
Procedimiento Gestión del Incidentes	01-01-SGSI

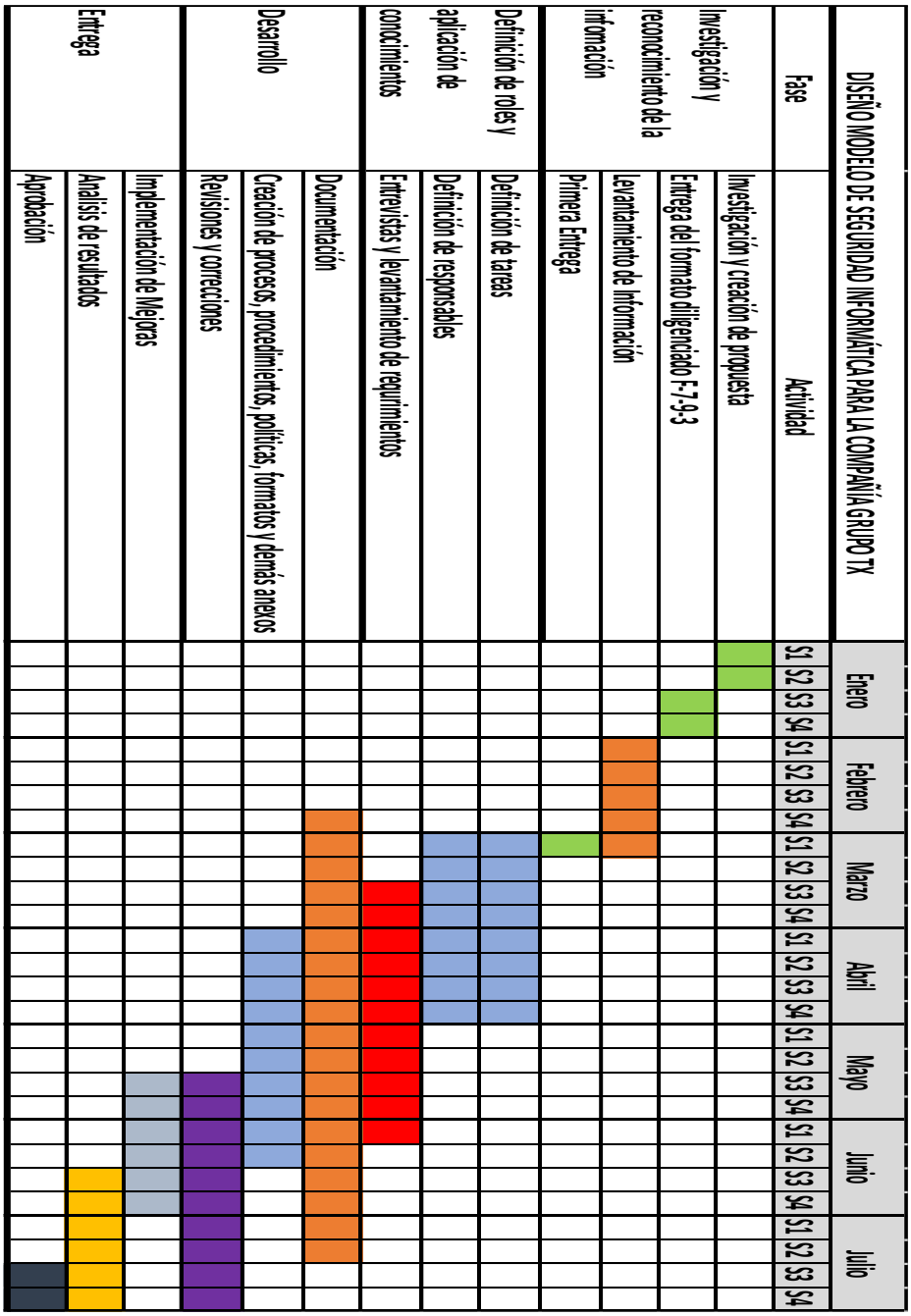
DOCUMENTOS DE REFERENCIA	**ORIGEN**		
DESCRIPCIÓN	**INTERNACIONAL**	**NACIONAL**	**INTERNO**
Norma Técnica Internacional 9001:2008 / Norma Internacional 27001	**X**		

Fuente: El Autor

ANEXO C

CRONOGRAMA GENERAL

Tabla C1. Cronograma General



Fuente: El Autor.

ANEXO D

CRONOGRAMA BACKUPS

Tabla D1. Cronograma Backup

Grupo Tx	PLANILLA PROGRAMACIÓN DE BACKUPS

DEPENDENCIA	TIPO	ENERO				FEBRERO				MARZO				ABRIL				MAYO				JUNIO				JULIO				AGOSTO				SEPTIEMBRE				OCTUBRE				NOVIEMBRE				DICIEMBRE				OBSERVACIONES
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	
GERENCIA GENERAL	INFORMACION																																															
	CORREO																																															
COMERCIAL	INFORMACION																																															
	CORREO																																															
ADMINISTRATIVA	INFORMACION																																															
	CORREO																																															
FINANCIERA	INFORMACION																																															
	CORREO																																															
SISTEMAS Y TECONOLOGIA	INFORMACION																																															
	CORREO																																															
OTROS	INFORMACION																																															
	CORREO																																															

ELABORO REVISO APROBO

Fuente: El Autor.

ANEXO E

CRONAGRAMA MANTENIMIENTO PREVENTIVO

Tabla E1. Cronograma Mantenimiento Preventivo.

Grupo Tx	CRONOGRAMA MANTENIMIENTOS PREVENTIVOS

No.	Proceso / Dependencia	CARGO	EQUIPO		REFERECIA DEL EQUIPO	ESTADO		PERIODICIDAD	FECHA PROGRAMACION	VERIFICACION AL CUMPLIMIENTO
			Portatil	Desktop		NUEVO	USADO			

Responsable del proceso

Gerencia General

Fuente: El Autor.

ANEXO F

POLÍTICA DE SEGURIDAD GRUPO TX

Tabla F1. Política de Seguridad.

Grupo Tx	**POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN**	Código: 01-01-POL-SGSI Versión: 01 Fecha: 25 de junio de 2020 Página: 1 de 6

CONTENIDO

Pág

1. OBJETIVO

Asegurar la buena gestión de la información de la compañía, mitigando y gestionando el riesgo al que puede estar expuesto. Cubriendo diferentes tipos de riesgos como en el aspecto legal, el sabotaje, fraude, estafa, extorsión, espionaje, robo o pérdida de activos, denegación de servicios, toma de decisiones correctas, destrucción de activos.

Garantizar que Grupo TX tenga una gestión de riesgos adecuada y que este modelo contribuya al negocio como un facilitador.

2. ALCANCE

La política de seguridad de la información se aplica a todos los procesos de la compañía que de alguna manera gestiona información relevante para el negocio, es por eso que es lo mismo que el proceso de tecnología y sistemas es transversal a todos los procesos de la agencia. Y tiene toda la aprobación de la alta gerencia para ser un elemento de control, que debe cumplirse para lograr objetivos estratégicos y misionales.

Se aplica a todo el personal de la compañía, proveedores y clientes que están relacionados con la misma.

Se aplica a toda la plataforma tecnológica, incluido cualquier equipo que se conecte o interactúe con la red de la agencia.

3. DEFINICIONES

- **SGSI.** Sistema de gestión de seguridad de la información.
- **Confidencialidad.** El uso que se le da a la información para dejar a disposición de ingresos y accesos no autorizados a ella.
- **Integridad.** Es la conservación de la información sin ningún tipo de modificación que alterar su exactitud en todo lo que le concierne.
- **Disponibilidad.** Cuando se tiene acceso a la información y los sistemas que interactúan con ella, habla de su disponibilidad.
- **Gestión de riesgos.** Es un método para determinar, analizar, evaluar y clasificar el posible riesgo, para luego implementar medidas de seguridad para controlarlo.
- **Vulnerabilidad.** Se entiende como una debilidad que ocurre en un sistema informático.
- **Amenaza**. Es cualquier evento que puede causar daños a un sistema de información y que causa pérdidas de cualquier tipo.
- **Incidentes de seguridad**. Es cualquier evento no deseado, que puede resultar en la interrupción de los servicios prestados por un sistema informático, un incidente se considera como la materialización de una amenaza.
- **Copia de seguridad.** Copia de seguridad. Significa duplicar la información contenida en la computadora o servidor, en una unidad de almacenamiento para anticipar la pérdida de la información debido a errores graves del sistema.

4. POLÍTICAS

1. Siempre y sin excepción, las medidas de seguridad se deben utilizar en la información independientemente del medio en el que se almacena o la forma en que se procesa.
2. Toda la información que de alguna manera es parte de la compañía, debe protegerse teniendo en cuenta su nivel de criticidad.
3. Los usuarios de Grupo TX acuerdan no divulgar, exhibir, revelar, mostrar, comunicar, usar y / o utilizar la información con ninguna persona natural o jurídica en su nombre o en nombre de terceros.
4. El uso de la información de la compañía no puede utilizarse por ningún motivo en detrimento de la organización.
5. Los equipos entregados para cumplir con las tareas diarias de carácter ocasional (presentaciones a clientes y otros), son temporales, por lo tanto, las presentaciones, documentos y otros archivos almacenados temporalmente deben eliminarse para evitar el uso malicioso y preservar la confidencialidad. del mismo.
6. Los usuarios serán autenticados con nombre de usuario y contraseña, lo que los hace directamente responsables del manejo de la información por este medio.
7. La información registrada en medios electrónicos, físicos o magnéticos pertenece a la compañía, por lo que los usuarios deben darle una gestión y uso adecuados de acuerdo con los intereses de la empresa, permitiendo la continuidad en la relación con el cliente.
8. La distribución, copia o eliminación de los archivos de los sistemas de información se realizará con autorización previa de la organización.
9. Al ser el uso de los computadores portátiles algo ocasional, es obligación del Usuario eliminar la información almacenada para evitar el uso malicioso de la información y preservar su confidencialidad.

10. Las contraseñas serán asignadas en el servidor de dominio por el administrador, que les dará un grado de complejidad.
11. Los usuarios deben realizar un cambio en la contraseña, solicitando la colaboración del administrador con respecto a los parámetros de seguridad necesarios.
12. La contraseña debe cambiarse periódicamente cada 45 días.
13. Las cuentas de correo electrónico deben asignarse a los usuarios con la solicitud previa del departamento de Recursos Humanos.
14. El servidor no guardará los mensajes del cliente de correo electrónico durante más de 60 días.
15. Es el compromiso de los usuarios purgar la información contenida en el correo web como en el cliente de correo electrónico.
16. Las cuentas de los usuarios que se retiran de la compañía, deben eliminarse mediante planificación, según el informe proporcionado por Recursos Humanos.
17. Las cuentas asignadas por la Grupo TX no deben usarse para tareas fuera de los objetivos de la compañía.
18. Los correos electrónicos enviados por los usuarios deben tener la firma institucional otorgada por el área de diseño.
19. El usuario debe abstenerse de acceder, guardar o distribuir material ilegal o no relacionado con el trabajo utilizando los medios electrónicos, físicos o magnéticos de la compañía.
20. Los usuarios no deben abrir, enviar o responder correos electrónicos considerados basura, spam o de remitentes desconocidos, para evitar el riesgo de virus, entre otros.
21. La información de la compañía, de interés general, se divulgará a través del sitio web y los canales autorizados.

22. De acuerdo con las pautas ofrecidas por los administradores de sistemas informáticos, se guardarán las copias de seguridad de la información del equipo informático, incluidos los correos electrónicos.
23. Las computadoras portátiles no tienen respaldo de datos ya que manejan información temporal que debe ser eliminada por el usuario.
24. El uso de Internet debe estar directamente relacionado con la misión de la compañía.
25. Los funcionarios del área sistemas y tecnología autorizados serán aquellos que permitan la conexión a la red inalámbrica.
26. Sin licenciamiento, los usuarios deben abstenerse de descargar desde los equipos de cómputo de la compañía material musical o videos de ningún tipo.
27. Los administradores de sistemas y tecnología asignados cambiarán periódicamente las claves correspondientes al uso de la red inalámbrica.

Las demás políticas, procesos, procedimientos, formatos y registros que forman parte del SGSI de la compañía, son parte integral de esta política de seguridad de la información.

Cumplimiento.

Este documento ha sido aprobado por la alta gerencia, para lo cual el incumplimiento o violación de esta política tendrá acciones disciplinarias, de acuerdo con lo estipulado en los contratos establecidos en cada situación. Las acciones legales también podrían aplicarse según corresponda.

No debe haber excepciones de ningún tipo en la aplicación de medidas de tratamiento de riesgos de información.

5. RESPONSABILIDADES

El Gerente General y / o Director de sistemas y tecnología, así como el trabajador designado, son responsables de la operación de la Infraestructura Tecnológica de la Compañía.

6. DOCUMENTOS DE REFERENCIA

DESCRIPCIÓN	ORIGEN		
	INTERNACIONAL	NACIONAL	INTERNO
Norma Técnica Internacional ISO 9001 / ISO 27001	X		

7. DESCRIPCIÓN DE CAMBIOS

VERSIÓN	FECHA VIGENCIA	DESCRIPCIÓN DE CAMBIOS
1		N/A

8. ANEXOS

ANEXO No.	NOMBRE
N/A	N/A

DIVULGACIÓN DEL DOCUMENTO.

El documento será divulgado a todos los procesos de la compañía.

ELABORO (Firma y Cargo):	REVISO (Firma y Cargo): Gerente General	APROBÓ (Firma y Cargo): Alta Gerencia

V.1

Fuente: El Autor.

ANEXO G

PLAN DE CAPACITACIÓN

Tabla G1. Plan de Capacitación

Grupo Tx	PLAN DE CAPACITACIÓN	Código: 01-01-SGSI-07 Versión: 01 Fecha: 27 de junio de 2020 Página: 1 de 1

PLAN DE CAPACITACIÓN

El plan de capacitación se compone de los temas principales que deben exponerse a los colaboradores de la Grupo TX, con respecto al proceso de gestión de riesgos, y se ejecutará de acuerdo con el cronograma establecido por la alta gerencia y reflejado en el formato de capacitación 01-01- SGSI -05.

Módulo 1	Módulo 2	Módulo 3
Política de Seguridad Grupo TX	**Buenas Prácticas en Seguridad de la Información**	**Manejo Eficiente de la infraestructura tecnológica de Grupo TX**
✓ Qué es una política de seguridad de la información. ✓ Por qué es importante conocerla. ✓ Política de Seguridad Grupo TX. ✓ Proceso de Gestión del riesgo. ✓ Deberes y Derechos.	✓ Dispositivos externos como USB'S. ✓ Contraseñas. ✓ Navegadores. ✓ Copias de Seguridad. ✓ Competencias de usuarios TIC	✓ Conocer la infraestructura. ✓ Licenciamiento de la compañía. ✓ Mesa de ayuda. ✓ Tratamiento a incidentes.
6 horas	**3 horas**	**6 horas**

Se propone una segunda fase de capacitación, para fortalecer las competencias de los usuarios, de acuerdo con los resultados obtenidos en la primera capacitación.

Módulos adicionales, según los requerimientos del negocio, se propone profundizar en la identificación de incidentes (Mesa de ayuda)

ELABORO (Firma y Cargo):	REVISO (Firma y Cargo): Gerente General	APROBÓ (Firma y Cargo): Alta Gerencia

V.1

Fuente: El Autor.

ANEXO H

PLANILLA GENERAL

Tabla H1. Planilla Servicio o Incidentes

Grupo Tx	PLANILLA GENERAL DE ASIGNACIÓN Y ATENCIÓN DE SERVICIOS O INCIDENTES												
No.	FECHA	AREA SOLICITANTE	NOMBRE DEL SOLICITANTE	SERVICIO SOLICITADO/ INCIDENTE	MEDIO DE SOLICITUD	RESPONSABLE DE PROCESO	APROBADO		RESPONSABLE DE APROBACIÓN	SERVICIO INTERNO O EXTERNO		OBSERVACIONES	ESTADO DE SERVICIO
							SI	NO					

Fuente: El Autor.

ANEXO I

PLANILLA CAPACITACIÓN

Tabla I1. Planilla Capacitación

Grupo Tx	PLANILLA DE CAPACITACIÓN

DETALLE CAPACITACIÓN								
Fecha dd/mm/aaaa	PROCESO	Nombre y Cargo	Tema de Capacitación	Material	Asistencia		Firma Usuario	Firma Responsable Capacitación
					SI	NO		

Nombre y Firma Responsable	Observaciones

Fuente: El Autor.

ANEXO J

PLANILLA BACKUP

Tabla J1. Planilla Backup

Grupo Tx	PLANILLA DE BACKUP

DETALLE BACKUP										
Fecha dd/mm/aaaa	Proceso	Nombre y Cargo	Referencia del Equipo	Directorio o Instancia	Tamaño (MB o GB)	Rótulo Medio Magnético	Envía a Custodia		Firma del Responsable del Equipo	Firma Responsable Custodia
							SI	NO		

Nombre y Firma Responsable	Observaciones

Fuente: El Autor.

ANEXO K

PROCEDIMIENTO DE GESTIÓN DE INCIDENTES GRUPO TX

Tabla K1. Procedimiento de Incidentes

Grupo Tx	**PROCEDIMIENTO DE GESTIÓN DE INCIDENTES**	Código: 01-01-SGSI-01 Versión: 01 Fecha: 01 de Julio de 2020 Página: 1 de 8

CONTENIDO

1. OBJETIVO

Administrar la gestión de incidentes en el área de sistemas y tecnología, garantizar la integridad, disponibilidad y confidencialidad de la información.

2. ALCANCE

Se aplica a todo el personal de la compañía, comienza con la necesidad de salvaguardar y garantizar los principios de seguridad informática y termina con la custodia y / o satisfacción de los requisitos que tienen que ver con la información de la organización.

3. DEFINICIONES

Almacenamiento. Bajo este término genérico, se agrupan los dispositivos y el software dedicados a archivar datos e información. Existen diferentes tipos de dispositivos de almacenamiento: discos, disquetes, discos ópticos, cintas, cartuchos, etc. Cada uno de ellos tiene ventajas y desventajas, y son más o menos adecuados para diferentes usos. En el caso de la informática, los dispositivos de almacenamiento más comunes son discos duros o fijos, memorias, disquetes o disquetes (de diferentes tamaños estandarizados), CD y DVD,

Copia de seguridad. Copia de seguridad. Significa duplicar la información contenida en la computadora o servidor, en una unidad de almacenamiento para anticipar la pérdida de la información debido a errores graves del sistema.

Base de datos (DataBase). Conjunto de datos relacionados que se almacenan de manera que se pueda acceder fácilmente, con la posibilidad de relacionarlos, ordenarlos en función de diferentes criterios, etc.

Servidor. Es el equipo central en un sistema de red que proporciona servicios a todos los nodos.

Sistema operativo (S.O.). Software básico que controla una computadora. El sistema operativo entre sus funciones es: coordinar datos, administrar, implementar y respaldar su entorno informático de manera eficiente.

Incidentes de seguridad. Es cualquier evento no deseado que puede resultar en la interrupción de los servicios prestados por un sistema informático, un incidente se considera la materialización de una amenaza

4. RESPONSABILIDADES

El Gerente General y / o director de sistemas y tecnología, así como el trabajador designado, son responsables de la operación de la Infraestructura Tecnológica de Grupo TX.

5. GENERALIDADES

5.1 Información

La información a la que se hace referencia en este documento es la producida o modificada en los procesos de la compañía, que se ha generado utilizando los recursos de Grupo TX o de acuerdo con los roles o responsabilidades de los trabajadores.

El objetivo es definir las condiciones y términos para disponer de la información de propiedad de Grupo TX a clientes externos e internos del proceso.

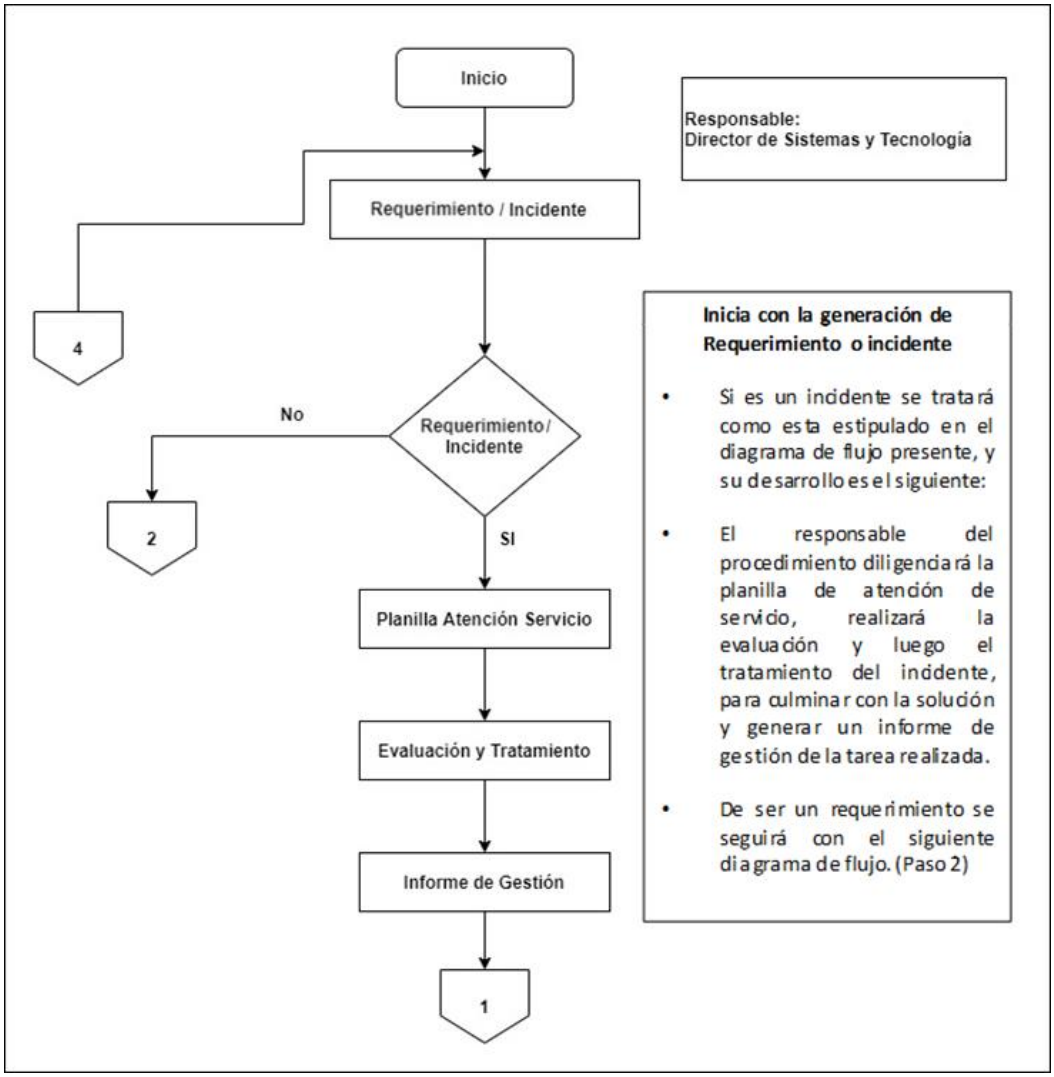
La entrega de la información de la compañía a otras entidades e individuos solo se puede hacer si hay una solicitud formal y previamente aprobada por el Gerente General y / o el director de sistemas y tecnología.

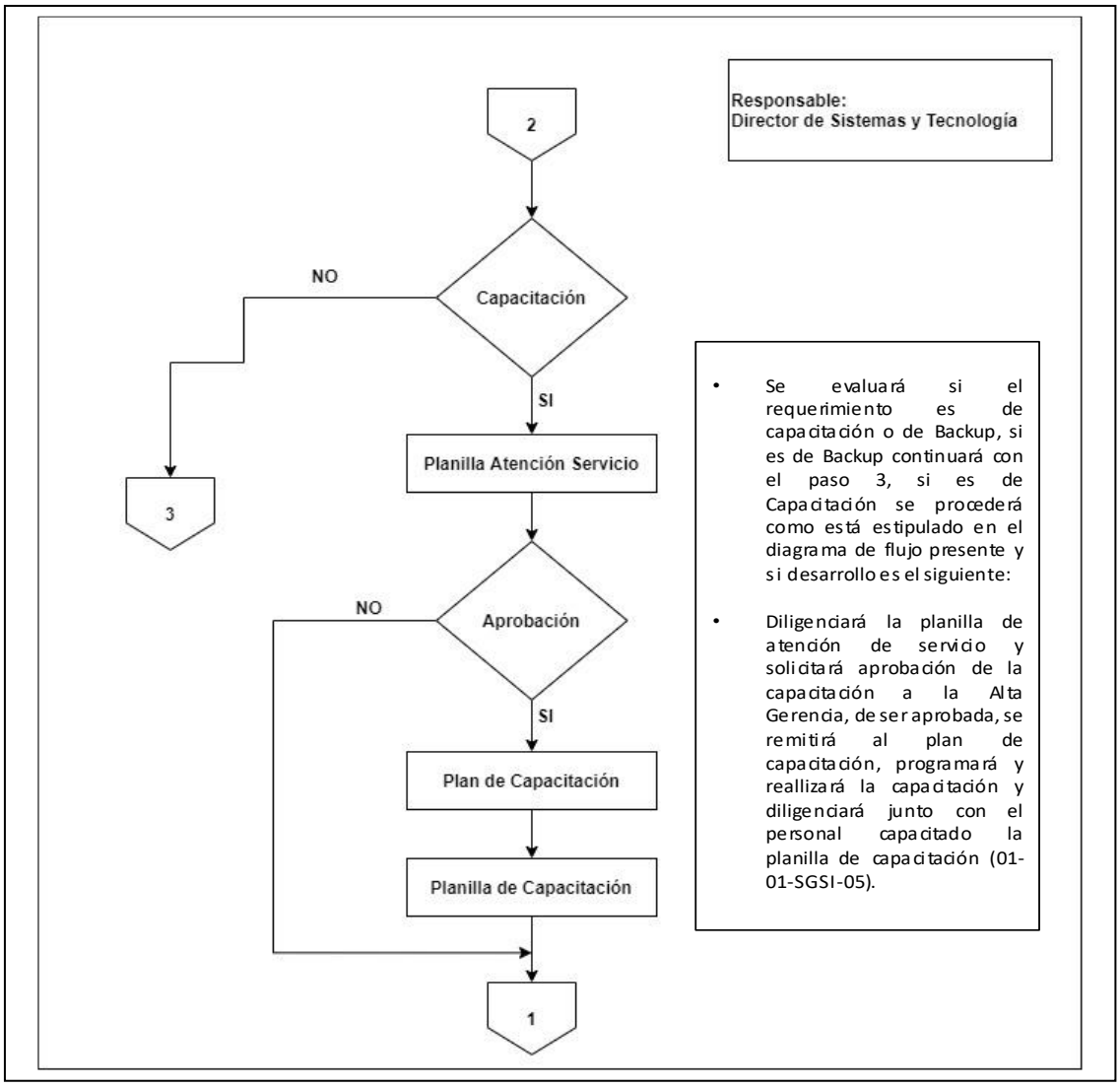
Está totalmente prohibido entregar información de manera informal en respuesta a solicitudes verbales, siempre debe haber un soporte físico. El uso que las entidades le dan a la información de Grupo TX está sujeto a los derechos de propiedad que la Compañía tiene sobre ella.

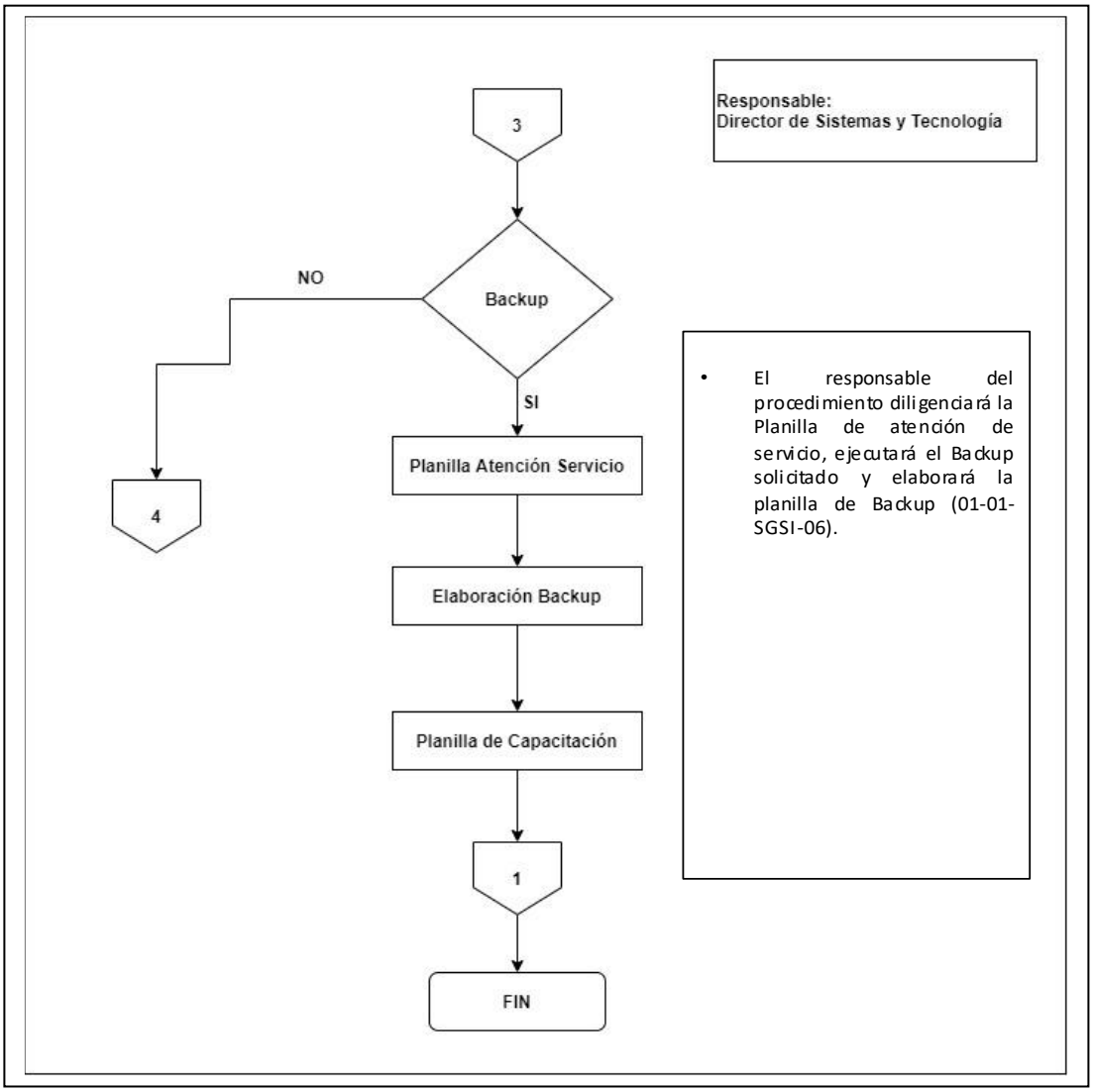
6. REGISTROS

Clase	Título del Documento	Código	Disposición
Formato	Solicitud formal del requerimiento /Incidente	01-01-SGSI-03	Se conserva en medio físico y magnético
Formato	Planilla General de Asignación y Atención de Servicio	01-01-SGSI-04	Se conserva en medio físico y magnético
Formato	Plan de Capacitación	01-01-SGSI-05	Se conserva en medio físico y magnético
Formato	Planilla de Backup	01-01-SGSI-06	Se conserva en medio físico y magnético
Registro	Informe de Presentación de Gestión	N.A.	Se conserva en medio físico y magnético

7. DESARROLLO




Responsable:
Director de Sistemas y Tecnología
2
Capacitación
NO
SI
3
Planilla Atención Servicio
Aprobación
NO
SI
Plan de Capacitación
Planilla de Capacitación
1
Se evaluará si el requerimiento es de capacitación o de Backup, si es de Backup continuará con el paso 3, si es de Capacitación se procederá como está estipulado en el diagrama de flujo presente y si desarrollo es el siguiente:
Diligenciará la planilla de atención de servicio y solicitará aprobación de la capacitación a la Alta Gerencia, de ser aprobada, se remitirá al plan de capacitación, programará y reallizará la capacitación y diligenciará junto con el personal capacitado la planilla de capacitación (01-01-SGSI-05).


3
Responsable:
Director de Sistemas y Tecnología
Backup
NO
SI
4
Planilla Atención Servicio
Elaboración Backup
Planilla de Capacitación
1
FIN
• El responsable del procedimiento diligenciará la Planilla de atención de servicio, ejecutará el Backup solicitado y elaborará la planilla de Backup (01-01-SGSI-06).

TIEMPO DE EJECUCIÓN	
RANGO MÍNIMO	**RANGO MÁXIMO**
2 Meses	1 Año

8. DOCUMENTOS DE REFERENCIA

DESCRIPCIÓN	ORIGEN		
	INTERNACIONAL	NACIONAL	INTERNO
Norma Técnica Internacional ISO 9001 / ISO 27001	X		

9. DESCRIPCIÓN DE CAMBIOS

VERSIÓN	FECHA VIGENCIA	DESCRIPCIÓN DE CAMBIOS
1		N/A

10. ANEXOS

ANEXO No.	NOMBRE
N/A	N/A

ELABORO (Firma y Cargo):	REVISO (Firma y Cargo): Garantía General	APROBÓ (Firma y Cargo): Alta Gerencia

Fuente: El Autor.

ANEXO L

SOLICITUD FORMAL DE REQUERIMIENTO INCIDENTE

Tabla L1. Solicitud Requerimiento o Incidente

Grupo Tx	SOLICITUD FORMAL DEL REQUERIMIENTO / INCIDENTE	Consecutivo No.

FECHA: _____ PROCESO SOLICITANTE : _____

NOMBRE DEL SOLICITANTE : _____

TIPO DE SOLICITUD

☐ 1. Instalaciones y demas ☐ 2. Capacitación ☐ 3. Cuentas de Acceso/Usuario

☐ 4. Incidente de seguridad ☐ 5. Backup de Información ☐ 6. Entrega de Información

ESPECIFICACIONES (Descripción del Incidente y/o requerimiento)

Aprobación:

FIRMA RESPONSABLE DE PROCESO

Gerente General y/o Director de Sistemas y Tecnología

FECHA PROYECTADA DE RESPUESTA: _____

01-01-GI-03
V.1

Fuente: El Autor.