PROYECTO

Diagnóstico de la Gestion de Acceso de Usuarios en la Superintendencia de Servicios Publicos Domiciliarios-

Norma ISO/IEC 27001:2013 Numerales A.9.2.2 y A.9.3.1

UNIVERSIDAD LIBRE DE COLOMBIA

FACULTAD DE INGENIERA

TRABAJO DE GRADO PARA OPTAR EL TITULO DE:

Especialista en Gerencia de Calidad en productos y servicios

Presentado por:

Ana Milena Parra Carrero

Ingeniera Telemática

Bogotá D.C.

Mayo de 2017

UNIVERSIDAD LIBRE DE COLOMBIA

FACULTAD DE INGENIERA

Presentado por:

Ana Milena Parra Carrero

Ingeniera Telemática

Presentado A:

Álvaro Jiménez

Ing. Industrial

Bogotá D.C.

Junio de 2017

CONTENIDO

TABLA DE ILUSTRACIONES

ÍNDICE DE TABLAS

CAPITULO I

INTRODUCCIÓN

La seguridad genera confianza al momento de realizar cualquier labor que desempeñemos teniendo en cuenta que determina dentro del ser humano confianza al momento hacer cualquier actividad personal o dentro de la vida laboral.

En la superintendencia de servicios públicos es un factor muy importante, toda vez que se maneja y almacena información de los prestadores de servicios públicos a nivel nacional, razón por la cual se ha determinado que la seguridad de la información dentro y fuera de la entidad genera confianza.

La seguridad de la información dentro de la entidad no hace mucho tiempo no era un factor importante, tal vez no por falta de conocimiento sino porque no se había implementado de la mejor manera la Norma ISO/IEC 27001:2013 de 2006, con su respectiva política de seguridad.

Adicionalmente, como los sistemas de información internamente han venido funcionando bien a lo largo de los años no se le había dado la suficiente importancia ya que se tiene la perspectiva que si las cosas no fallan, se encuentran funcionando de la mejor manera.

Por tal razón, a nivel gubernamental el ministerio de las telecomunicaciones, A través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, dando cumplimiento a sus funciones, a través de las cuales contribuye a la construcción de un Estado más eficiente, más transparente y participativo, expone el modelo de seguridad y privacidad de la información, para dar cumplimiento a lo establecido en el componente de seguridad y privacidad de la información de la estrategia de gobierno en línea.

Razón por la cual, se pretende realizar el estudio de la implementación de la Norma ISO/IEC 27001:2013 de 2006 – Anexo 9.2 Norma Seguridad de la Información, dentro de la superintendencia de servicios públicos en acompañamiento del Ingeniero Hernán Muriel – Funcionario de la Superintendencia de servicios públicos, quien es la persona encargada del área de seguridad de la información y es la persona que ha venido realizando los diagnósticos e implementación de la norma desde el año 2014.

GENERALIDADES

ANTECEDENTES

A través de los años el avance de la tecnología tanto en las empresas como las entidades gubernamentales sean dado a la tarea de implementar herramientas que les ayuden a mantener y cuidar la información que se considere importante dentro de la organización, toda vez que se cuenta con personas que pretendan alterar dicha información y utilizarla de manera mal intencionada o simplemente se consideren los datos tan valiosos que debamos cuidarlos y mantenerlos seguros. Razón por la cual sea implementada la seguridad de la información.

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la **información** buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.

Según **la norma 27001:2013 indica que la seguridad de la información** consiste en asegurar que los recursos del Sistema de Información de una empresa se utilicen de la forma que ha sido decidido y el acceso de información se encuentra contenida, así como controlar que la modificación solo sea posible por parte de las personas autorizadas para tal fin y por supuesto, siempre dentro de los límites de la autorización.

Los objetivos de la seguridad informática:

Los activos de información son los elementos que la **Seguridad de la Información** debe proteger. Por lo que son tres elementos lo que forman los activos:

- Información: es el objeto de mayor valor para la empresa o entidad.
- Equipos: suelen ser software, hardware y la propia organización.
- Usuarios: son las personas que usan la tecnología de la organización.

Como características básicas de la seguridad informática se encuentra:

- ✓ Identificar el peligro:
- ✓ Darle una clasificación: alto, medio, bajo
- ✓ Determinar cuál es la mejor forma de protegernos en cuanto a ese peligro.

Esto con el fin de poder buscar una protección de los datos y buscar protegernos frente a las amenazas o peligros y poder minimizar riesgos relacionados con estos.

El decreto 1078 de 2015, por medio del cual se expide el decreto único reglamentario del sector de tecnologías de información y las comunicaciones, en el TITULO 9, POLÍTICAS Y LINEAMIENTOS DE TECNOLOGÍAS DE LA INFORMACIÓN, CAPITULO 1, Estrategia de Gobierno en Línea - GEL, en la SECCIÓN 2, COMPONENTES, INSTRUMENTOS Y RESPONSABLES, se define el componente de seguridad y privacidad de la información, como parte integral de la estrategia GEL, y es de obligatorio cumplimiento para las entidades del estado como lo establece en la sección 3, MEDICIÓN, MONITOREO Y PLAZOS.

La estrategia de Gobierno en Línea, liderada por el Ministerio TIC, tiene como objetivo, garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones,

con el fin de contribuir con la construcción de un Estado más participativo, más eficiente y más transparente. Para el desarrollo del componente de Seguridad y Privacidad de la Información, se ha diseñado un documento de lineamientos "Modelo de Seguridad y Privacidad de la Información" el cual a lo largo de los últimos años, ha sido utilizado por las diferentes entidades tanto del orden nacional y territorial, como guía para mejorar

Los estándares de seguridad de la información, de acuerdo con las nuevas tendencias tecnológicas, este documento se ha ido actualizando de acuerdo con las modificaciones de la norma técnica que le sirve de sustento para el modelo la NTC-ISO 27001:2013-2006, las mejores prácticas y los cambios normativos que tengan impacto sobre el mismo.

El Modelo de Seguridad y Privacidad de la Información se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión.

Con el fin de facilitar la apropiación del modelo y su correcta implementación en las entidades, se propone esta nueva versión que recoge además de los cambios técnicos de la norma, herramientas específicas de privacidad relacionadas con las normas y los retos que el nuevo marco normativo (Ley de datos personales, Transparencia y Acceso a la Información Pública, entre otras), las cuales se deben tener en cuenta para la gestión de la información, así como los lineamientos que permiten la adopción del protocolo IPv6 en el Estado Colombiano. }

Finalmente, a nivel metodológico se debe recordar que han incluido una serie de guías en cada una de las fases del modelo, para que los destinatarios del mismo tengan claridad de que información se desea y como registrarla en el sistema para que sea más amigable a la mayoría de personas (persona del común)

PLANTEAMIENTO DEL PROBLEMA

DESCRIPCIÓN DEL PROBLEMA

La capacidad actual del Estado para enfrentar las amenazas cibernéticas presenta debilidades y no existe una estrategia nacional al respecto. A partir de ello se establecen las causas y efectos que permitirán desarrollar políticas de prevención y control, ante el incremento de amenazas informáticas. Para la aplicabilidad de la estrategia se definen recomendaciones específicas a desarrollar por entidades involucradas directa e indirectamente en esta materia. Así lo ha entendido el Gobierno Nacional al incluir este tema en el Plan Nacional de Desarrollo 2010-2014 “Prosperidad para Todos”, como parte del Plan Vive Digital (CONPES 3701,2011).

La superintendencia de servicios públicos no es ajena a este problema, a través de los años ha tratado de implementar un sistema de seguridad de la información que permita a todas aquellas personas interactuar con la plataforma informática (www.superservicios.gov.co / www.sui.gov.co) de forma segura según lo establece la normatividad vigente por medio de Gobierno en línea, pero por los diferentes problemas evidenciados como falta de una política clara referente a seguridad de la información y falta de estándares de calidad para verificar la calidad de la información, en la SSPD, específicamente en el grupo SUI donde se hace el análisis de la información oficial aportada por los prestadores no se hace una revisión exhaustiva de la calidad y seguridad en términos de la legislación referente a este tema.

Dentro de este documento se traza como meta central de esta política el fortalecimiento de la capacidad del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético, y a su vez se definen tres objetivos específicos:

1) Implementar instancias apropiadas para prevenir, atender, controlar y generar recomendaciones que regulen los incidentes y/o emergencias cibernéticas para proteger la infraestructura crítica nacional;

2) Diseñar y ejecutar planes de capacitación especializada en ciberseguridad ; y

3) Fortalecer el cuerpo normativo y de cumplimiento en la materia (CONPES 3701,2011), basados en la Norma NTC-ISO 27001:2013-2006.

PLANTEAMIENTO DEL PROBLEMA

La Superintendencia de Servicios Públicos Domiciliarios viene presentando deficiencias en cuanto a la seguridad de la información porque no se cuenta con un sistema de gestión de la calidad de la información optimo que satisfaga los requerimientos legales que son necesarios para el cumplimiento de las metas por ejemplo el registro de los prestadores de servicios públicos dentro del Sistema Único de Información.

Basados en la Guía 5 política general de Gobiernos en Línea y en la NTC 27001:2013 se pretende dar solución a este problema basados en la estructura definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información en la Superintendencia de Servicios Públicos, buscando obtener unos lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza

fortaleciendo la articulación entre los protocolos de seguridad de la información Ipv4 a Ipv6 haciendo uso de tres conceptos: análisis, planeación e implementación que orientará a las entidades del gobierno y a la sociedad en general a la seguridad de la información. Teniendo en cuenta el anexo 9.2 de la Norma ISO/IEC 27001:2013, que hace referencia a los requisitos básicos necesarios para diagnosticar, implementar y mantener el sistema de seguridad de la información en la entidad específicamente.

OBJETIVOS

Determinar y asegurar los controles de acceso de los usuarios autorizados y denegar el acceso a los no autorizados, establecidos en la política de seguridad de la información de la entidad.

OBJETIVO GENERAL

Estructurar el modelo de seguridad de la información aplicando la norma NTC ISO /IEC 27001:2013, tomando como guía el anexo 9.2, implementando controles, monitoreo y seguimiento en la plataforma de la SSPD.

OBJETIVOS ESPECÍFICOS:

- Analizar y realizar un diagnóstico de seguridad en el acceso de usuarios autorizados con los que se cuenta actualmente la Superintendencia de Servicios Públicos.

- Definir procesos apropiados para prevenir, atender, controlar y generar derechos de acceso para los sistemas y servicios con los que se cuenta actualmente en la Superservicios.

- Establecer controles que permitan restringir los derechos con los que cuentan los usuarios que tienen acceso a la información a la Superservicios.

JUSTIFICACIÓN

Un sistema de gestión de seguridad de la información bien implementado dentro de la entidad le permitirá demostrar y demostrarse a si mismo que cumple con sus valores misionales toda vez que se encuentra comprometida y cumple sus objetivos estratégicos, ya que estaría gestionando eficientemente los riesgos a los que se encuentra expuesta. Adicionalmente le permitirá a la entidad en general fortalecer integralmente las relaciones entre áreas ya que existiría un nivel alto de confianza.

Realizando un diagnóstico adecuado de la implementación de un nuevo protocolo en cuanto a la seguridad de la información en la SSPD, la información que se publica deberá cumplir con los estándares de Norma ISO/IEC 27001:2013 y las normas del ministerio TIC, es importante tener en cuenta que no solo será implementado en la SSPD sino en todas las entidades Gubernamentales, teniendo en cuenta que se pretende minimizar el riesgo de los procesos misionales de la entidad, Cumplir con los principios de seguridad de la información, cumplir con los principios de la función administrativa , Mantener la confianza de los funcionarios, contratistas y terceros, apoyar la innovación tecnológica, implementar el sistema de gestión de seguridad de la información , proteger los activos de información, establecer las políticas, procedimientos e instructivos en materia de seguridad de la información , fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la superintendencia de servicios públicos y así garantizar la continuidad del negocio frente a incidentes que se lleguen a presentar.

Asegurar la información clave en el contexto empresarial, en un mundo altamente interconectado, basado en redes sociales y con sobrecarga de información (particularmente instantánea), es un reto para cualquier ejecutivo de seguridad de la información.

En este sentido, entender la dinámica corporativa y la forma como la inseguridad de la información se materializa es una competencia estratégica que los responsables de la seguridad de la información deben desarrollar para mantenerse alertas y anticiparse a los movimientos de la inevitabilidad de la falla. Para ello, este libro ofrece referentes básicos de pensamiento estratégico en seguridad de la información, fundado en su concepto par: la inseguridad de la información, entendido como elemento práctico de gobierno corporativo que permite a los estrategas de la seguridad de la información pensar de manera complementaria y generar escenarios alternos a los tradicionales para superar el síndrome de la “falsa sensación de seguridad”. (M., Jeimy J. Cano, 2014)

La seguridad de la información es muy reciente. Sus implicaciones van desde el análisis forense de un incidente común de pérdida o de ocultamiento de información en un computador personal, hasta aspectos de defensa nacional. La acción de malware puede afectarnos en cualquier momento. Cuando nos adelantamos en el ciberterrorismo y en la guerra en el ciberespacio, pasando por aquellos escenarios más característicos de un crimen, en este caso, con el uso de la informática. (M., Jeimy J. Cano, 2014)

1.5 DELIMITACIÓN

El diagnostico de seguridad informática se realizará a nivel general de la entidad, con respecto al uso de contraseñas, manejo de backups, estandarización de procesos para la administración de hardware y software y el control de accesos. Estos son los cuatro puntos más importantes en la organización a los cuales se les harán el respectivo diagnóstico y seguimiento dado que son los que se pretenden fortalecer en la entidad.

El levantamiento de la información se utilizará el método de observación directa y entrevistas a los diferentes encargados de la parte de software y comunicaciones. Para abordar el primer punto que se refiere al uso de contraseñas, se utilizará el método de encuesta y se llevarán a cabo pruebas que demuestren la vulnerabilidad de las mismas y la facilidad para acceder a los sistemas de información y al mismo sistema operativo.

1.5.1 Espacio

En las instalaciones de la Superintendencia de Servicios Públicos, dentro del subproceso del Grupo SUI-(Sistema Único de Información), el cual hace parte del proceso de Informática - sede Calle 85 (Cra 18 – 84 – 35) Piso 2. Basado en la norma NTC-ISO/ IEC 27001:2013, donde se realizar el análisis y diagnóstico de la seguridad de la información de la entidad basados en el anexo 9.2 de la mencionada norma.

1.5.2 Tiempo

Los plazos para la implementación de las actividades se establecieron para el Manual de Gobierno en Línea, y a través del Decreto 2573 de 2014, en el Articulo 10. "Plazos. Los sujetos obligados deberán implementar las actividades establecidas en el Manual de Gobierno en Línea dentro de los siguientes plazos, el proyecto inicio estudios a comienzos del 2015, fase que aún no está terminada pero que requería el 25% de su ejecución para iniciar con la lluvia de ideas y aplicaciones en busca de resultados en el 2016, el proyecto busca solo hasta el 2017 validar los resultados de las ideas que se propongan.

Sujetos Obligados del Orden Nacional Componente/Año	2015	2016	2017	2018	2019
Planear TIC para ser servicios (SSPD)	18%	25%	30%	50%	Mantener 100%
Implementar TIC para Gobierno abierto (SSPD)	20%	30%	30%	50%	Mantener 100%
Ejecutar TIC	15%	20%	20%	50%	Mantener 100%

para la Gestión (SSPD)					
Realizar seguimiento a Seguridad y Privacidad de la Información (SSPD)	25%	60%	60%	50%	Mantener 100%

Tabla 1: Cronograma

Fuente: Guía 9 - Indicadores Gestión de Seguridad de la Información - http://www.mintic.gov.co/gestionti/615/articles-5482_G9_Indicadores_Gestion_Seguridad.pdf

El cronograma de actividades se comenzó en el año 2015, pero nos Tabla 1: Cronograma le ha dado la suficiente importancia al tema de la implementación teniendo en cuenta que como es una entidad gubernamental como falencia vital se encuentra la rotación de personal que cuando asumen el proyecto modifican el trabajo anteriormente hecha sufriendo un retroceso en las actividades realizadas, razón por la cual el avance a través del tiempo ha sido casi nulo.

1.5.3 Contenido

La política dentro de la norma NTC ISO 27001:2013 de 2006, se centra en la formación del personal en temas relacionados con la seguridad de la información dentro de la Superservicios, cuya finalidad es disminuir las vulnerabilidades y amenazas relacionadas con el recurso humano aplicando un nuevo protocolo que vaya acorde con la tecnología de punta en Colombia. Dado que

el alcance de la entidad es a nivel nacional.

1.5.4 Política De Seguridad Informática

La Superintendencia de Servicios Públicos Domiciliarios comprometida con la integridad, confidencialidad y disponibilidad de la información, identifica y reduce los riesgos, relacionados con la divulgación, modificación, destrucción o uso indebido de los activos de información de la entidad.

(http://sigme.superservicios.gov.co/sigme-calidad/CALIDAD/MECI/CODIGO%20DE%20ETICA%20Y%20BUEN%20GOBIERNO/CODIGO_ETICA_Y_BUEN_GOBIERNO.pdf)

1.6 MARCO REFERENCIAL

1.6.1 MARCO TEÓRICO.

SUPERINTENDENCIA DE SERVICIOS PUBLICOS DOMICILIARIOS

La Superintendencia de Servicios Públicos Domiciliarios, Superservicios, es un organismo de carácter técnico, creado por la Constitución de 1991, que, por delegación del Presidente de la República de Colombia, ejerce inspección, vigilancia y control las entidades y empresas prestadoras de servicios públicos domiciliarios.

Misión

Somos una entidad técnica que contribuye al mejoramiento de la calidad de vida en Colombia, mediante las funciones de vigilancia, inspección y control en relación con la prestación de los servicios públicos domiciliarios, la protección de los derechos y la promoción de los deberes de los usuarios y responsabilidades de los prestadores.

Visión

Seremos a 2019 una entidad técnica reconocida nacional e internacionalmente por su gestión frente a las funciones de vigilancia inspección y control a la prestación de los servicios públicos

domiciliarios, así como en la implementación de las mejores prácticas en la administración pública, comprometidos con la excelencia, por sus altos estándares de desempeño

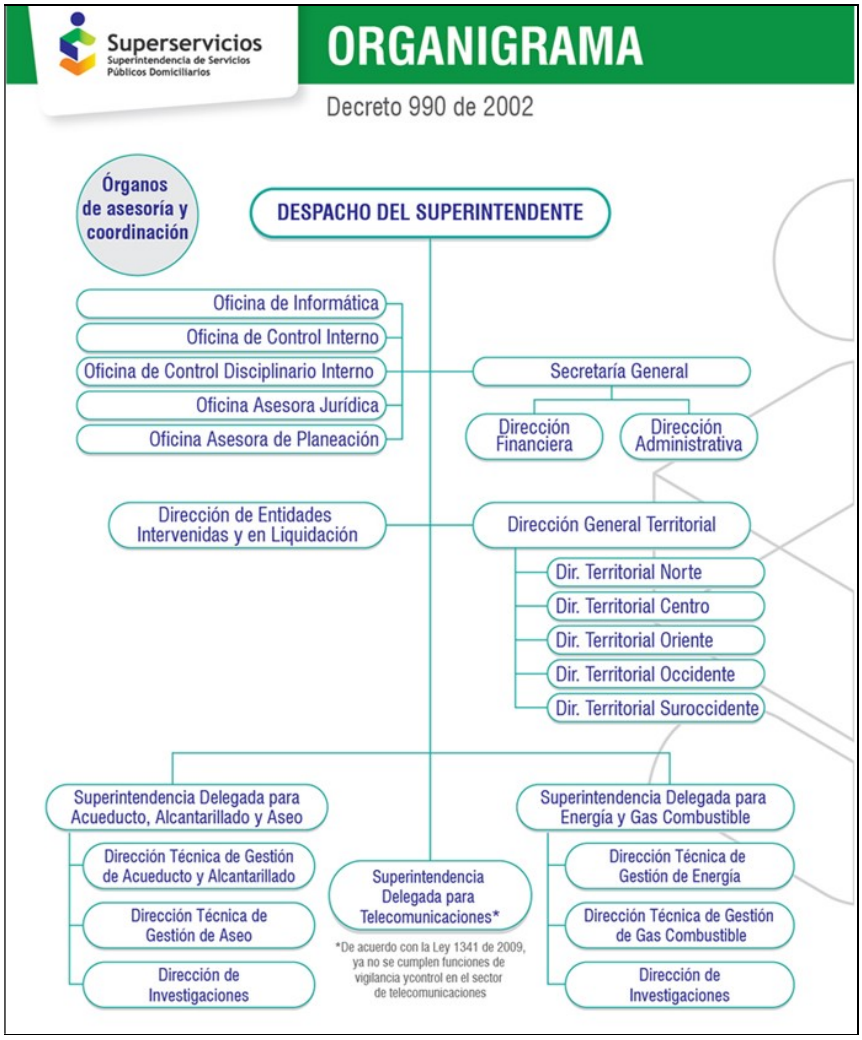

Ilustración 1: Organigrama

Fuente: La entidad

1.6.1.1 Norma ISO/IEC

El Organismo Internacional de Normalización (ISO) fue creado en 1947 y cuenta con 91 estados miembros, que son representados por organismos nacionales de normalización. Dicho organismo trabaja para lograr una forma común de conseguir el establecimiento del sistema de calidad, que garantice la satisfacción de las necesidades y expectativas de los consumidores.

Las normas ISO se crearon con la finalidad de ofrecer orientación, coordinación, simplificación y unificación de criterios a las empresas y organizaciones con el objeto de reducir costes y aumentar la efectividad, así como estandarizar las normas de productos y servicios para las organizaciones internacionales.

Las normas ISO se han desarrollado y adoptado por multitud de empresas de muchos países por una necesidad y voluntad de homogeneizar las características y los parámetros de calidad y seguridad de los productos y servicios.

1.6.1.2 Norma ISO/IEC 27001:2013

ISO 27001:2013 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

El Anexo A.9.2 Gestión de acceso de usuarios de la Norma ISO/IEC 27001 y 9.3.1uso de información de autenticidad secreta, contiene los diferentes objetivos de control y controles que las organizaciones deberían tener en cuenta para la planeación e implementación de su Sistema de Gestión de Seguridad de la Información, los cuales se describen en la Norma ISO/IEC 27002, objeto de estudio **http://iso27000.es/iso27002.html**

ISO/IEC 27002. Guía de buenas prácticas en seguridad de la información describe de forma detallada los objetivos de control y controles descritos de una forma general en el Anexo A.9.2 Gestión de acceso de usuarios de la Norma ISO/IEC 27001.

ISO/IEC 27003. Guía que contiene aspectos necesarios para el diseño e implementación de un Sistema de Gestión de Seguridad de la Información de acuerdo a los requerimientos establecidos en la Norma ISO/IEC/IEC 27001, describe de forma clara y detallada el proceso desde la planeación hasta la puesta en marcha de planes de implementación.

ISO/IEC 27004. Guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un Sistema de Gestión de Seguridad de la Información y de los objetivos de control y controles implementados de acuerdo al Anexo A.9.2 Gestión de acceso de usuarios de la Norma ISO/IEC 2700113.

ISO/IEC 27005. Establece los lineamientos para la gestión de riesgos de seguridad de la información y está diseñada para ayudar a las organizaciones en la implementación de un Sistema de Gestión de Seguridad de la Información basada es un enfoque de gestión de riesgos.

ISO/IEC 27006. Establece los requisitos relacionados en la Norma ISO/IEC 27001 que deben cumplir las organizaciones para la acreditación de entidades de auditoría y certificación de Sistemas de Gestión de Seguridad de la Información.

ISO/IEC 27035. Proporciona una guía sobre la gestión de incidentes de seguridad en la información

1.6.1.3 Necesidad de la Seguridad de la Información

La implementación del sistema de gestión de calidad dentro de la Superservicios surge de la necesidad de asegurar la información que se almacena dentro de la entidad, toda vez que dicha información corresponde a la i formación que suministran las empresas de servicios públicos a nivel nacional en cuanto a las operaciones de cada una de ellas. La Superservicios con dicha información se encarga de vigilar y controlar la prestación de los servicios públicos domiciliarios.

Por cuanto, es de vital importancia que la Superservicios implemente un sistema de seguridad de información que le permita estar protegido a los ataques que pueda llegar a estar expuestos, teniendo en cuenta que no es favorable y conveniente que dicha información sea vulnerada o alterada por terceros.

1.6.1.4 Información

La información es un recurso que, como el resto de los importantes activos comerciales, tiene valor para una organización y por consiguiente debe ser debidamente protegida. La seguridad de la información protege ésta de una amplia gama de amenazas, a fin de garantizar la continuidad institucional, minimizar el daño y maximizar el retorno sobre las inversiones y las oportunidades.
La información puede existir en muchas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, presentada en imágenes, o expuesta en una conversación. Cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada.

La seguridad de la información se define aquí como la preservación de las siguientes características:

- **Confidencialidad:** se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a ella.
- **Integridad:** se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- **Disponibilidad:** se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con ella toda vez que se requiera.

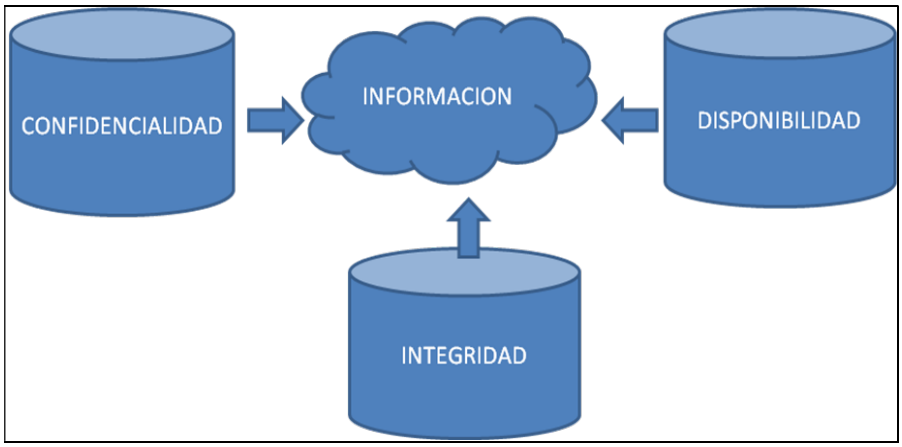

Ilustración 2: Seguridad de la Información

Fuente: Autor

1.6.1.5 Seguridad Informática

Considerar aspectos de seguridad significa

a) conocer el peligro,

b) clasificarlo y

c) protegerse de los impactos o daños de la mejor manera posible.

Esto significa que solamente cuando estamos conscientes de las potenciales amenazas, agresores y sus intenciones dañinas (directas o indirectas) en contra de nosotros, podemos tomar medidas de protección adecuadas, para que no se pierda o dañe nuestros recursos valiosos, la Seguridad Informática sirve para la protección de la información, en contra de amenazas o peligros, para evitar daños y para minimizar riesgos, relacionados con ella.

1.6.1.6 Sistema de Gestión de Seguridad de la Información

El SGSI es la abreviatura usada para referirse al Sistema de Gestión de la Seguridad de la Información e ISMS son las siglas equivalentes en ingles a Information Security Management System.

Podemos entender por información todo el conjunto de datos que se organizan en una organización y otorgan valor añadido para ésta, de forma independiente de la forma en la que se guarde o transmita, el origen que tenga o la fecha de elaboración.

El Sistema de Gestión de Seguridad de la Información, según ISO 27001 consiste en preservar la confidencialidad, integridad y disponibilidad, además de todos los sistemas implicados en el tratamiento dentro de la organización.

Según el conocimiento que se tiene del ciclo de vida de la información relevante se puede adoptar la utilización de un proceso sistemático, documentado y conocido por toda la empresa, desde un enfoque de riesgos empresarial. El proceso es el que constituye un **SGSI**.

1.6.1.7 Utilización:

La información, junto a los procesos y los sistemas que hacen uso de ella, son activos demasiado importantes para la empresa. La **confidencialidad, integridad y disponibilidad** de dicha información puede ser esencial para mantener los niveles de competitividad, conformidad, rentabilidad e imagen de la empresa necesarios para conseguir los objetivos de la empresa y asegurase de que haya beneficios económicos.

Las empresas y los sistemas de información se encuentran expuestos a un número cada vez más elevado de amenazas que aprovechan cualquier tipo de vulnerabilidad para someter a los activos críticos de información a ataques, espionajes, vandalismo, etc. Los virus informáticos o los ataques son ejemplos muy comunes y conocidos, pero también se deben asumir los riesgos de sufrir incidentes de seguridad que pueden ser causados voluntariamente o involuntariamente desde dentro de la propia empresa o los que son provocados de forma accidental por catástrofes naturales.

El cumplimiento de la legislación, la adaptación dinámica y de forma puntual de todas las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar que se obtiene el máximo beneficio son algunos de los aspectos fundamentales en los que un **SGSI** es una herramienta de gran utilidad y de importante ayuda para la gestión de las empresas.

El nivel de seguridad que se alcanza gracias a los medios técnicos es limitado e insuficiente por sí mismo. Durante la gestión efectiva de la seguridad debe tomar parte activa toda la empresa, con la gerencia al frente, tomando en consideración a los clientes y a los proveedores de la organización.

El modelo de gestión de la seguridad tiene que contemplar unos procedimientos adecuados y planificar e implementar controles de seguridad que se basan en una evaluación de riesgos y en una medición de la eficiencia de los mismos.

Para entender **que es SGSI,** ayuda a establecer la política de seguridad y los procedimientos en relación a los objetivos de negocio de la empresa, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir. *blog editado por ISOTools Excellence (2005). SGSI es una iniciativa de ISOTools Excellence sobre la Seguridad de la Información. recuperado http://www.pmg-ssi.com/norma-27001/*

1.6.1.8 Beneficios

- Establecer una metodología de **Gestión de la Seguridad** estructurada y clara.
- Reducir el riesgo de pérdida, robo o corrupción de la información sensible.
- Los clientes tienen acceso a la información mediante medidas de seguridad.
- Los riesgos y los controles son continuamente revisados.
- Se garantiza la confianza de los clientes y los socios de la organización.
- Las auditorías externas ayudan de forma cíclica a identificar las debilidades del **SGSI** y las áreas que se deben mejorar.
- Facilita la integración con otros sistemas de gestión.
- Se garantiza la continuidad de negocio tras un incidente grave.
- Cumple con la legislación vigente sobre información personal, propiedad intelectual y otras.
- La imagen de la organización a nivel internacional mejora.
- Aumenta la confianza y las reglas claras para las personas de la empresa.
- Reduce los costes y la mejora de los procesos y el servicio.
- Se incrementa la motivación y la satisfacción del personal.

- Aumenta la seguridad en base la gestión de procesos en lugar de una compra sistemática de productos y tecnologías.

La documentación mínima que se debe tener en cuenta a la hora de implementar un **SGSI**:

- Política y objetivos de seguridad.
- El alcance del **SGSI**.
- Los procedimientos y los controles que apoyan al **SGSI**.
- Describir toda la metodología a la hora de realizar una evaluación de riesgo.
- Generar un informe después de realizar la evaluación de riesgo.
- Realizar un plan de tratamiento de riesgos.
- Procedimientos de planificación, manejo y control de los procesos de **seguridad de la información** y de medición de la eficacia de los controles.
- Declaración de aplicabilidad.
- Procedimiento de gestión de toda la documentación del **SGSI**.

1.6.1.9 Gestión de Riesgo en la Seguridad Informática

La Gestión de Riesgo es un método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo.

En su forma general contiene cuatro fases:

- **Análisis**: Determina los componentes de un sistema que requiere protección, sus vulnerabilidades que lo debilitan y las amenazas que lo ponen en peligro, con el resultado

de revelar su grado de riesgo.

- **Clasificación**: Determina si los riesgos encontrados y los riesgos restantes son aceptables.
- **Reducción**: Define e implementa las medidas de protección. Además, sensibiliza y capacita los usuarios conforme a las medidas.
- **Control**: Analiza el funcionamiento, la efectividad y el cumplimiento de las medidas, para determinar y ajustar las medidas deficientes y sanciona el incumplimiento.

Todo el proceso está basado en las llamadas políticas de seguridad, normas y reglas institucionales, que forman el marco operativo del proceso, con el propósito de:

- Potenciar las capacidades institucionales, reduciendo la vulnerabilidad y limitando las amenazas con el resultado de reducir el riesgo.
- Orientar el funcionamiento organizativo y funcional.
- Garantizar comportamiento homogéneo.
- Garantizar corrección de conductas o prácticas que nos hacen vulnerables.
- Conducir a la coherencia entre lo que pensamos, decimos y hacemos.

Se debe distinguir entre los dos, porque forman la base y dan la razón, justificación en la selección de los elementos de información que requieren una atención especial dentro del marco de la Seguridad Informática y normalmente también dan el motivo y la obligación para su protección. Sin embargo, hay que destacar que, aunque se diferencia entre la Seguridad de la Información y la Protección de Datos como motivo u obligación de las actividades de seguridad, las medidas de protección aplicadas normalmente serán las mismas.

En la Seguridad de la Información el objetivo de la protección son los datos mismos y trata de evitar su perdida y modificación no-autorizado. La protección debe garantizar en primer lugar la confidencialidad, integridad y disponibilidad de los datos, sin embargo, existen más requisitos como por ejemplo la autenticidad entre otros.

El motivo o el motor para implementar medidas de protección, que responden a la Seguridad de la Información, es el propio interés de la institución o persona que maneja los datos, porque la pérdida o modificación de los datos, le puede causar un daño (material o inmaterial). Entonces en referencia al ejercicio con el banco, la pérdida o la modificación errónea, sea causado intencionalmente o simplemente por negligencia humana, de algún récord de una cuenta bancaria, puede resultar en pérdidas económicas u otras consecuencias negativas para la institución.

En el caso de la Protección de Datos, el objetivo de la protección no son los datos en sí mismo, sino el contenido de la información sobre personas, para evitar el abuso de esta.

Esta vez, el motivo o el motor para la implementación de medidas de protección, por parte de la institución o persona que maneja los datos, es la obligación jurídica o la simple ética personal, de evitar consecuencias negativas para las personas de las cuales se trata la información.

En muchos Estados existen normas jurídicas que regulan el tratamiento de los datos personales, como por ejemplo en España, donde existe la “Ley Orgánica de Protección de Datos de Carácter Personal” que tiene por objetivo garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas

físicas, y especialmente de su honor, intimidad y privacidad personal y familiar [1]. Sin embargo, el gran problema aparece cuando no existen leyes y normas jurídicas que evitan el abuso o mal uso de los datos personales o si no están aplicadas adecuadamente o arbitrariamente.

Existen algunas profesiones que, por su carácter profesional, están reconocidos u obligados, por su juramento, de respetar los datos personales como por ejemplo los médicos, abogados, jueces y también los sacerdotes. Pero independientemente, si o no existen normas jurídicas, la responsabilidad de un tratamiento adecuado de datos personales y las consecuencias que puede causar en el caso de no cumplirlo, recae sobre cada persona que maneja o tiene contacto con tal información, y debería tener sus raíces en códigos de conducta, y finalmente la ética profesional y humana, de respetar y no perjudicar los derechos humanos y no hacer daño.

La variedad, amplitud y complejidad de los sistemas de información que adquieren, requieren o encuentran disponibles las organizaciones actuales, junto a la dinámica del permanente cambio observado en las tecnologías de la información y las comunicaciones, han impulsado de múltiples formas y, al mismo tiempo, condicionado las grandes transformaciones de las organizaciones, los mercados y el mundo de la modernidad y de la posmodernidad. Son cambios que, además de sus innegables ventajas, han traído simultáneamente para las personas y las organizaciones, amenazas, riesgos y espectros de incertidumbre en los escenarios de internet, intranet, desarrollo tecnológico, gestión de la información, la comunicación y los sistemas (Álvarez-Marañón & Pérez-García, 2004, pp. 30-40).

Con cada vez mayor frecuencia y mayor impacto, los dispositivos de almacenamiento y procesamiento de información -llámense servidores, estaciones de trabajo o simplemente PC- son

vulnerados en sus elementos más sensibles, dejando expuestos no sólo múltiples y significativos datos de distinto valor (financiero, crediticio, estratégico, productivo...), sino los mismos patrimonios reales de personas y organizaciones y, aún más, su dignidad, su honra y su vida.

Con el avance de la tecnología informática y su influencia en casi todas las áreas de la vida social y empresarial, han surgido comportamientos ilícitos llamados de manera genérica *delitos informáticos*, que han abierto un amplio campo de riesgos y también de estudio e investigación, en disciplinas jurídicas y técnicas, pero especialmente en aquellas asociadas con auditoría de sistemas o auditoría informática.

De acuerdo con los estudios realizados por Cisco en 2008, según los cuales el país registraba una de las calificaciones más bajas en seguridad informática (62 puntos de 100 posibles), en comparación con otros seis países de Latinoamérica. Esa situación, que obedece a distintos factores, según concepto de algunos ejecutivos de firmas relacionadas con la informática y la auditoría (Etek, Cisco, Trend Micro), se explica en factores como:

- Falta de información, falta de claridad o debilidad en la gestión gerencial, referidos particularmente a la implementación de la seguridad informática.
- Abuso en el empleo de los sistemas y sus aplicativos.
- Ausencia de políticas claras sobre seguridad informática.
- Falta de reconocimiento estratégico al área de Auditoría de Sistemas.
- Falta de conciencia en el desempeño de los sistemas de información.
- Baja gestión y poco uso de herramientas de análisis y control.

- Falta de evaluación con relaciones beneficio/costo y criterios de continuidad del negocio, sobre uso y seguridad de la información y los recursos informáticos.

Según Manuel Bustos, director de la multinacional de seguridad de la información Etek: "La industria en general, el sector gobierno y las pymes son los menos preocupados por la seguridad de la información, porque requiere inversiones y normalmente no le dedican lo suficiente para lograr un nivel adecuado de seguridad" (Cisco, 2008).

1.6.1.10 Retos de da Seguridad

La eficiente integración de los aspectos de la Seguridad Informática en el ámbito de las organizaciones sociales centroamericanas enfrenta algunos retos muy comunes que están relacionados con el funcionamiento y las características de estas.

- Los temas transversales no reciben la atención que merecen y muchas veces quedan completamente fuera de las consideraciones organizativas: Para todas las organizaciones y empresas, la propia Seguridad Informática no es un fin, sino un tema transversal que normalmente forma parte de la estructura interna de apoyo. Nadie vive o trabaja para su seguridad, sino la implementa para cumplir sus objetivos.
- Carencia o mal manejo de tiempo y dinero: Implementar medidas de protección significa invertir en recursos como tiempo y dinero.
- El proceso de monitoreo y evaluación, para dar seguimiento a los planes operativos está deficiente y no integrado en estos: Implementar procesos y medidas de protección, para garantizar la seguridad, no es una cosa que se hace una vez y después se olvide, sino requiere un control continuo de cumplimiento, funcionalidad y una adaptación periódica,

de las medidas de protección implementadas, al entorno cambiante.

- Todas estas circunstancias juntas, terminan en la triste realidad, que la seguridad en general y la Seguridad Informática en particular no recibe la atención adecuada. El error más común que se comete es que no se implementa medidas de protección, hasta que después del desastre, y las escusas o razones del porque no se hizo/hace nada al respecto abundan.
- Enfrentarse con esta realidad y evitando o reduciendo los daños a un nivel aceptable, lo hace necesario trabajar en la "Gestión de riesgo ", es decir a) conocer el peligro, b) clasificarlo y c) protegerse de los impactos o daños de la mejor manera posible.

Pero una buena Gestión de riesgos no es una tarea única sino un proceso dinámico y permanente que tiene que estar integrado en los procesos (cotidianos) de la estructura institucional, que debe incluir a todas y todos los funcionarios y que requiere el reconocimiento y apoyo de las directiva. Sin estas características esenciales no están garantizados, las medidas de protección implementadas no funcionarán y son una pérdida de recursos.

1.6.1.11 Elementos de Información

Los Elementos de información son todos los componentes que contienen, mantienen o guardan información. Dependiendo de la literatura, también son llamados Activos o Recursos.
Son estos los Activos de una institución que tenemos que proteger, para evitar su perdida, modificación o el uso inadecuado de su contenido, para impedir daños para nuestra institución y las personas presentes en la información.

Generalmente se distingue y divide tres grupos

- Datos e Información: son los datos e informaciones en sí mismo
- Sistemas e Infraestructura: son los componentes donde se mantienen o guardan los datos e informaciones
- Personal: son todos los individuos que manejan o tienen acceso a los datos e informaciones y son los activos más difíciles de proteger, porque son móviles, pueden cambiar su afiliación y son impredecibles

1.6.1.12 Amenazas y Vulnerabilidades

Se presentan cuestiones del por qué el sistema puede sufrir amenazas y la vulnerabilidad que tiene ante las mismas.

Amenazas:

Una Amenaza es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el caso de la Seguridad Informática, los Elementos de Información. Debido a que la Seguridad Informática tiene como propósitos garantizar la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones, las amenazas y los consecuentes daños que puede causar un evento exitoso, también hay que ver en relación con la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones.

Desde el punto de vista de la entidad que maneja los datos, existen amenazas de origen

externo como por ejemplo las agresiones técnicas, naturales o humanos, sino también amenazas de origen interno, como la negligencia del propio personal o las condiciones técnicas, procesos operativos internos.

Generalmente se distingue y divide tres grupos

- Criminalidad: son todas las acciones, causado por la intervención humana, que violan la ley y que están penadas por esta. Con criminalidad política se entiende todas las acciones dirigido desde el gobierno hacia la sociedad civil.
- Sucesos de origen físico: son todos los eventos naturales y técnicos, sino también eventos indirectamente causados por la intervención humana.
- Negligencia y decisiones institucionales: son todas las acciones, decisiones u omisiones por parte de las personas que tienen poder e influencia sobre el sistema. Al mismo tiempo son las amenazas menos predecibles porque están directamente relacionado con el comportamiento humano.
- Existen amenazas que difícilmente se dejan eliminar (virus de computadora) y por eso es la tarea de la gestión de riesgo de preverlas, implementar medidas de protección para evitar o minimizar los daños en caso de que se realice una amenaza.

Vulnerabilidades:

La Vulnerabilidad es la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño. En otras palabras, es la capacitad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño.

Las vulnerabilidades están en directa interrelación con las amenazas porque si no existe una amenaza, tampoco existe la vulnerabilidad o no tiene importancia, porque no se puede ocasionar un daño.

Dependiendo del contexto de la institución, se puede agrupar las vulnerabilidades en grupos característicos: Ambiental, Física, Económica, Social, Educativo, Institucional y Política

Un estudio de ESET Latinoamérica estableció cuáles eran los males cibernéticos más frecuentes en las compañías y cuál es el panorama de seguridad informática en la región.
El análisis se realizó por medio de encuestas a 3.369 empresarios de Argentina, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Honduras, México, Nicaragua, Panamá, Paraguay, Perú y Venezuela.

Según la investigación, en el primer lugar están los ataques de malware (malicious software, que en español se conoce como código malicioso) afectando al 41% de las compañías. Este, el caso más frecuente para las empresas de América Latina, es un software que busca dañar los sistemas de información o el computador de un usuario.

Para los analistas encuestadores no fue una sorpresa que el malware sea la amenaza con mayor recurrencia ya que es un mal que viene aquejando al sector desde años atrás. Sin embargo, para el 2013, la cantidad de empresas infectadas disminuyó.

El segundo lugar es para el phishing que afectó durante 2013 al 17% de las empresas. Esta

modalidad es una suplantación de identidad con la que adquieren información confidencial.

La tercera y cuarta plaza están ocupadas por la falta de disponibilidad y la explotación de vulnerabilidades, dos modalidades que afectaron al 15% de las empresas y que hacen referencia al acceso de desconocidos a la seguridad de la empresa. Estas personas pueden, incluso, no ser expertos o hackers.

El top cinco lo cierra el ataque DoS, un ataque que dejó al 14% de las compañías con servicios o recursos inaccesibles para sus usuarios legítimos.

El sexto lugar fue para el acceso indebido, modalidad que afectó al 13% de las compañías, que como su nombre lo indica, hace referencia a la intromisión de terceros en información no pública.

El ranking lo finalizan el fraude interno que afectó al 10% de las empresas y el fraude externo que perjudicó al 9%.

Expertos de este estudio señalaron que las empresas se están preocupando por atacar los problemas que menos afectaciones causaron, dejando de lado medidas para evitar los casos de phishing o las infecciones de malware. Explican que el 68% de las empresas se preocupan por la explotación de vulnerabilidades, el 55% por infección de malware, el 44% por fraudes, el 38% por ataque DoS y el 37% por el phishing.

En Colombia, el 36% de las compañías fueron infectadas por malware, seguido por el 20%

afectado por la falta de disponibilidad. El 17% de las compañías colombianas fue víctima de phishing, el 14% de explotación de vulnerabilidades y el 10% de acceso indebido.

Los expertos recomendaron que no basta con hacer grandes inversiones en recursos de seguridad o sus departamentos de informática, sino que también deben concientizar y establecer controles sobre lo que se cuenta internamente en la compañía.

Recomiendan, también, no realizar actividades para prevenir incidentes cibernéticos con los trabajadores porque estos podrían incrementarse cuando ellos ya reconocen los controles habituales.

Agregan que es indispensable mejorar en las empresas la capacidad de reacción porque las políticas de seguridad, a pesar de estar tan definidas, no están acompañadas por prácticas de gestión frente a los incidentes menores. Por esto, señalan que deben aumentar la prioridad de este tipo de gestiones o la empresa quedaría indefensa.

Finalmente aconsejan hacer mayores campañas y actividades educativas para los empleados y considerar herramientas de análisis de riesgos para identificar los puntos más débiles de la estructura empresarial y que requieran de mayor atención.

1.6.1.13 Análisis de Riesgo

El primer paso en la Gestión de riesgo es el análisis de riesgo que tiene como propósito determinar los componentes de un sistema que requieren protección, sus vulnerabilidades que los

debilitan y las amenazas que lo ponen en peligro, con el fin de valorar su grado de riesgo.

La clasificación de datos tiene el propósito de garantizar la protección de datos (personales) y significa definir, dependiendo del tipo o grupo de personas internas y externas, los diferentes niveles de autorización de acceso a los datos e informaciones. Considerando el contexto de nuestra misión institucional, tenemos que definir los niveles de clasificación como por ejemplo: confidencial, privado, sensitivo y público. Cada nivel define por lo menos el tipo de persona que tiene derecho de acceder a los datos, el grado y mecanismo de autenticación.

Una vez clasificada la información, tenemos que verificar los diferentes flujos existentes de información internos y externos, para saber quiénes tienen acceso a qué información y datos.
Clasificar los datos y analizar el flujo de la información a nivel interno y externo es importante, porque ambas cosas influyen directamente en el resultado del análisis de riesgo y las consecuentes medidas de protección. Porque solo si sabemos quiénes tienen acceso a qué datos y su respectiva clasificación, podemos determinar el riesgo de los datos, al sufrir un daño causado por un acceso no autorizado.

Existen varios métodos de como valorar un riesgo y al final, todos tienen los mismos retos - las variables son difíciles de precisar y en su mayoría son estimaciones- y llegan casi a los mismos resultados y conclusiones.

En el ámbito de la Seguridad Informática, el método más usado es el Análisis de Riesgo.
La valoración del riesgo basada en la fórmula matemática

Riesgo = Probabilidad de Amenaza x Magnitud de Daño

Para la presentación del resultado (riesgo) se usa una gráfica de dos dimensiones, en la cual, el eje-x (horizontal, abscisa) representa la "Probabilidad de Amenaza" y el eje-y (vertical, ordenada) la "Magnitud de Daño". La Probabilidad de Amenaza y Magnitud de Daño pueden tomar condiciones entre Insignificante y Alta. En la práctica no es necesario asociar valores aritméticos a las condiciones de las variables, sin embargo, facilita el uso de herramientas técnicas como hojas de cálculo.

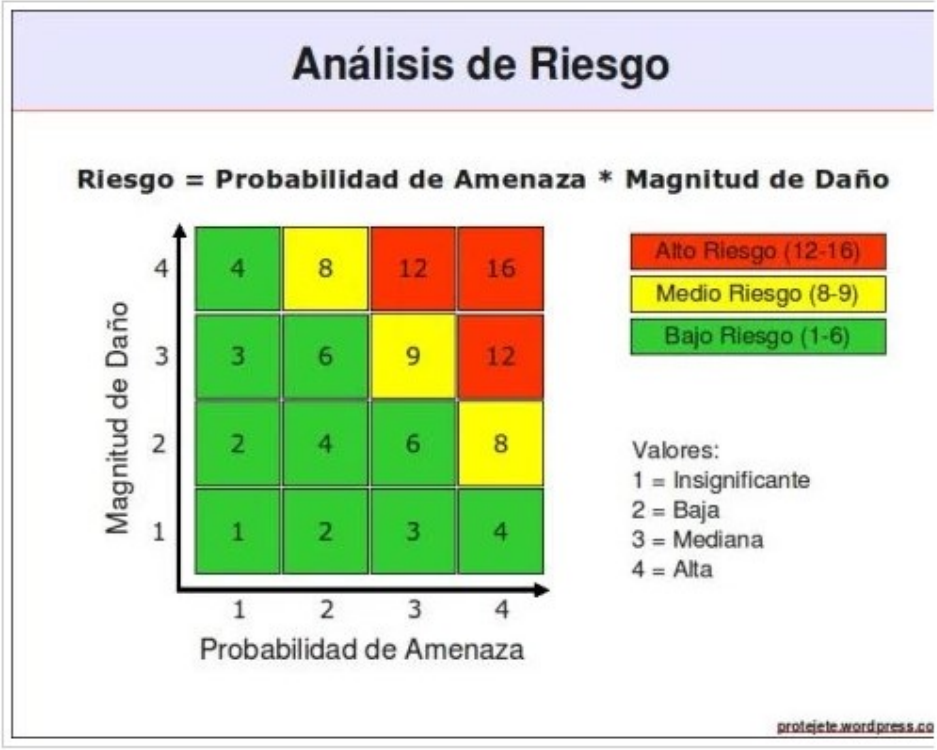

Ilustración 3: Figura 3. Gráfica Análisis de Riesgo más utilizado en el SGSI

Fuente**:** **https://protejete.wordpress.com/gdr_principal/analisis_riesgo/**

En el proceso de analizar un riesgo también es importante reconocer que cada riesgo tiene

sus características:

- Dinámico y cambiante (Interacción de Amenazas y Vulnerabilidad)
- Diferenciado y tiene diferentes caracteres (caracteres de Vulnerabilidad)
- No siempre es percibido de igual manera entre los miembros de una institución que tal vez puede terminar en resultados inadecuados y por tanto es importante que participan las personas especialistas de los diferentes elementos del sistema (Coordinación, Administración financiera, Técnicos, Conserje, Soporte técnico externo etc.).

El modelo se pude aplicar a los diferentes elementos de manera aislada, sino también al sistema completo, aunque en el primer caso, el resultado final será más preciso pero también requiere más esfuerzo.

Entre más alta la Probabilidad de Amenaza y Magnitud de Daño, más grande es el riesgo y el peligro al sistema, lo que significa que es necesario implementar medidas de protección.

1.6.1.14 Probabilidad de Amenaza

Se habla de un Ataque, cuando una amenaza se convirtió en realidad, es decir cuando un evento se realizó. Pero el ataque no dice nada sobre el éxito del evento y sí o no, los datos e informaciones fueron perjudicado respecto a su confidencialidad, integridad, disponibilidad y autenticidad.

1.6.1.15 Magnitud de Daño

Se habla de un Impacto, cuando un ataque exitoso perjudicó la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones.

Unas preguntas que se pueden hacer para identificar posibles consecuencias negativas causadas por un impacto son:

- ¿Existen condiciones de incumplimiento de confidencialidad (interna y externa)? Esto normalmente es el caso cuando personas no-autorizadas tienen acceso a información y conocimiento ajeno que pondrá en peligro nuestra misión.
- ¿Existen condiciones de incumplimiento de obligación jurídicas, contratos y convenios? No cumplir con las normas legales fácilmente puede culminar en sanciones penales o económicas, que perjudican nuestra misión, existencia laboral y personal.
- ¿Cuál es el costo de recuperación? No solo hay que considerar los recursos económicos, tiempo, materiales, sino también el posible daño de la imagen pública y emocional.

Considerando todos los aspectos mencionados, permite clasificar la Magnitud del Daño. Sin embargo, otra vez tenemos que definir primero el significado de cada nivel de daño (Baja, Mediana, Alta). (Gestión de Riesgo en la Seguridad Informática, 2014)

Un Sistema de Gestión de Seguridad de la Información (SGSI) es un conjunto de procesos que permiten establecer, implementar, mantener y mejorar de manera continua la seguridad de la información, tomando como base para ello los riesgos a los que se enfrenta la organización.

Su implantación supone el establecimiento de procesos formales y una clara definición de responsabilidades en base a una serie de políticas, planes y procedimientos que deberán constar

como información documentada.

1.6.1.16 Procesos

Fundamentalmente se distinguirán dos tipos de procesos**:**

- **Procesos de gestión.** Controlan el funcionamiento del propio sistema de gestión y su mejora continua.
- **Procesos de seguridad.** Se centran en los aspectos relativos a la propia seguridad de la información.

Con el Modelo de Seguridad para las entidades del Estado, el Ministerio TIC entrega una guía para que puedan construir su Sistema de Gestión de Seguridad de la Información (SGSI). Se busca generar una conciencia colectiva sobre la importancia de clasificar, valorar y asegurar los activos de cada entidad.

Por eso mismo, el Ministerio TIC está profundizando en elementos que permitan entender la realidad frente al proceso de implementación de SGSI en el Estado. Se debe forjar una línea base sobre cuáles son los motivadores, inhibidores, actores, resultados, entre otros aspectos, que cada entidad afronta en el camino hacia la seguridad de la información. Para tal fin, se ha contratado un estudio para "conocer cuál es el estado actual de adopción y apropiación de los SGSI en las entidades del Estado, del orden nacional y territorial".

"El proyecto de creación de un Sistema de Gestión de Seguridad de la Información, comienza

generalmente por el área de TI.

La mayoría plantea un alcance inicial que incluye mínimo el área de TI y los sistemas de información de la entidad.

Las razones para este tipo de alcance inicial son: practicidad y recursos".

Solo con la puesta en marcha del proyecto de adopción las entidades reconocen la importancia práctica del tema, la diferencia real entre SI y seguridad informática, hasta dónde pueden llegar en corto plazo y hasta dónde les gustaría llegar.

Las entidades son conscientes que el tema no sólo abarca el aseguramiento con software y hardware, si no que en gran medida el resultado exitoso se refleja en la sensibilización y compromiso del personal para cumplir cada política, conociendo el porqué de cada una. (Ministerio de Telecomunicaciones)

1.6.1.17 El Ciclo de Mejora Continúa

Ilustración 4: Ciclo PHVA

Fuente: https://www.google.com.co/search?q=imagen+del+ciclo+phva

Una novedad con respecto a anteriores versiones de la norma es la desaparición del ciclo PDCA como marco obligatorio para la gestión de mejora continua, indicando únicamente en su apartado 10.2 que "la organización debe mejorar de manera continua la idoneidad, adecuación y eficacia del sistema de gestión de seguridad de la información".

No obstante, el ciclo PDCA está implícito en la propia estructura de la norma, por lo que a continuación se desarrolla este modelo de mejora continúa que creemos que es necesario conocer. El modelo PDCA o "Planificar-Hacer-Verificar-Actuar" (Plan-Do-Check-Act, de sus siglas en inglés), consta de un conjunto de fases que permiten establecer un modelo comparable a lo largo

del tiempo, de manera que se pueda medir el grado de mejora alcanzado:

• Plan. En esta fase se planifica la implantación del SGSI. Se determina el contexto de la organización, se definen los objetivos y las políticas que permitirán alcanzarlos. Se correspondería con los capítulos 4, 5, 6 y 7 de la Norma UNEISO/IEC 27001:2013.

• Do. En esta fase se implementa y pone en funcionamiento el SGSI. Se ponen en práctica las políticas y los controles que, de acuerdo al análisis de riesgos, se han seleccionado para cumplirlas. Para ello debe de disponerse de procedimientos en los que se identifique claramente quién debe hacer qué tareas, asegurando la capacitación necesaria para ello. Se correspondería con el capítulo 8 de la Norma UNE-ISO/IEC 27001:2013

• Check. En esta fase se realiza la monitorización y revisión del SGSI. Se controla que los procesos se ejecutan de la manera prevista y que además permiten alcanzar los objetivos de la manera más eficiente. Se correspondería con el capítulo 9 de la Norma UNE-ISO/IEC 27001:2013

• Act. En esta fase se mantiene y mejora el SGSI, definiendo y ejecutando las acciones correctivas necesarias para rectificar los fallos detectados en la anterior fase. Se correspondería con el capítulo 10 de la Norma UNE-ISO/IEC 27001:2013

A la hora de diseñar el SGSI, se debe tener en cuenta que sobre el mismo se aplicará un proceso de mejora continua, con lo que conviene partir de una primera versión del mismo adaptado a las necesidades, operativas y recursos de la organización, con unas medidas de seguridad mínimas que permitan proteger la información y cumplir con los requisitos de la norma. Así, el SGSI será mejor adoptado por las personas implicadas, evolucionando de manera gradual y con un menor esfuerzo

En octubre de 2013 se publicaban las revisiones de las normas internacionales ISO/ IEC 27001:2013 (adoptada como norma española en 2014) e ISO/IEC 27002 (adoptada como norma española en 2015) que sustituían a las versiones de 2005.

Como se ha comentado anteriormente, esta norma internacional es una de las primeras en adoptar el Anexo SL, mejorando así la integración con otros sistemas de gestión. Presenta además otras diferencias con respecto a la anterior versión:

- Aparece la figura del propietario del riesgo. Se enfatiza así la importancia de gestionar riesgos y oportunidades en lugar de activos.
- No establece cómo se deben evaluar los riesgos. En la anterior norma se especificaba la necesidad de identificar activos, amenazas y vulnerabilidades, pero en esta nueva versión únicamente se hace referencia a "identificar los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información".

Ahora, la identificación de activos, amenazas y vulnerabilidades es una opción para la evaluación de riesgos, pero se pueden aplicar otras alternativas, haciéndose referencia a la Norma UNE-ISO 31000 Gestión del riesgo.

1.6.1.18 Principios y Directrices.

Desaparecen las referencias a documentos y registros, pasándose a hablar de información

documentada, que podrá estar en cualquier soporte (papel o electrónico).

- Se modifica el enfoque en cuanto a la actividad de selección de controles. En anteriores versiones de la norma, se seleccionaban los controles del Anexo A.9.2 Gestión de acceso de usuarios que permitiesen reducir los riesgos a un nivel aceptable. En esta versión el proceso sería: inicialmente, determinar los controles que se necesitan (sin tomar ningún marco como referencia) y posteriormente comparar los controles determinados con el Anexo A.9.2 Gestión de acceso de usuarios para asegurarse de que no se ha olvidado ninguno.
- Se eliminan las acciones preventivas, ya que estas se consideran acciones derivadas de la gestión de riesgos.
- Se actualiza el conjunto de controles, pasando de 133 repartidos en 11 secciones, a 114 repartidos en 14 secciones. Aparecen nuevos controles y desaparecen otros cuyo contenido se reparte, evitando así anteriores duplicidades.

Los requisitos de la Norma UNE-ISO/IEC 27001:2013, al igual que sucede con otros sistemas de gestión, son aplicables a todo tipo de organizaciones, independientemente de su naturaleza, tamaño o sector de actividad.

Esta norma específica los requisitos para establecer, implementar, mantener y mejorar de manera continua un SGSI, teniendo en cuenta los objetivos y riesgos de la organización. No obstante, no concreta cómo deben llevarse a cabo estos procesos, existiendo diversas posibilidades de dar cumplimiento a los mismos. Por ejemplo, establece las características que debe cumplir el proceso de evaluación de riesgos, pero no concreta la metodología ni los métodos a seguir. Esto ofrece a la organización flexibilidad a la hora de definir la manera de dar cumplimiento a los

requisitos, ajustándolos a su naturaleza y capacidad.

La Norma UNE-ISO/IEC 27002 incluye un catálogo de buenas prácticas, desarrolladas En base a la experiencia y colaboración de numerosos participantes, que han alcanzado un consenso acerca de los objetivos generalmente aceptados para la implantación y gestión de la seguridad de la información.

Los objetivos de control y los controles de esta norma internacional sirven de guía para la implantación de las medidas de seguridad. Por ello, la selección de los controles se realizará en función de los resultados de un proceso previo de evaluación de riesgos, y el grado de implementación de cada control se llevará a cabo de acuerdo a las necesidades de seguridad identificadas y a los recursos disponibles de la organización, buscando un equilibrio entre seguridad y coste.

Por otra parte, según la revista Dinero en su artículo sobre actualidad Las crecientes necesidades de Cyberseguridad dan a conocer que Un mundo cada vez más sistematizado, conectado y digital obedece a la necesidad de ser un mundo más inteligente. Las soluciones de cyberseguridad están para afrontar los riesgos y los problemas que ese mundo también representa.

Es un hecho real que la piratería informática hoy preocupa a los Estados, las empresas y a los ciudadanos. Los últimos estudios de seguridad en el mundo afirman que *hoy, éste delito, es el segundo de mayor alcance en el mundo después del narcotráfico.*

Las herramientas de seguridad se orientan a servir como barrera de protección contra

ataques cibernéticos. Los desafíos empresariales son aún más complejos y requieren que las entidades construyan las capacidades automáticas de orquestar y manejar todas las herramientas de una organización bajo un "celebro" centralizado. Sin embargo, muchas veces las empresas no evolucionan hacia sistemas nuevos y más robustos pues consideran que el que tienen supuso una gran inversión y que uno diferente no se podrá integrar. ***Sin autor. (2015). Las crecientes necesidades de Cyberseguridad. Dinero.com, recuperado de http://www.dinero.com/actualidad/articulo/las-crecientes-necesidades-cyberseguridad/215059***.

1.6.2 MARCO CONCEPTUAL

Validando que las identificaciones del problemas y la delimitación con el entorno nos dan un campo más exacto se pretende buscas acciones que permitan corregir el actual estado de fallas y a futuro su prevención, para permitir ver y aprovechar las oportunidades que dicha información almacenada traen a la organización.

Acción correctiva: Acción para eliminar la causa de una no conformidad y prevenir su repetición. Va más allá de la simple corrección.

Acción preventiva: Medida de tipo pro-activo orientada a prevenir potenciales no conformidades. Es un concepto de ISO 27001:2013:2005. En ISO 27001:2013:2013, ya no se emplea; ha quedado englobada en Riesgos y Oportunidades.

Aceptación del riesgo: Decisión informada de asumir un riesgo concreto.

Activo: (inglés: Asset). En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

Alcance: (Inglés: Scope). Ámbito de la organización que queda sometido al SGSI.

Amenaza: (inglés: Threat). Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Análisis de riesgos: (Inglés: Risk analysis). Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Análisis de riesgos cualitativo: (Inglés: Qualitative risk analysis). Análisis de riesgos en el que se usa algún tipo de escalas de valoración para situar la gravedad del impacto y la probabilidad de ocurrencia.

Análisis de riesgos cuantitativo: (Inglés: Quantitative risk analysis). Análisis de riesgos en función de las pérdidas financieras que causaría el impacto.

Auditor: (inglés: Auditor). Persona encargada de verificar, de manera independiente, el cumplimiento de unos determinados requisitos.

Auditor de primera parte: (Inglés: *First party auditor*). Auditor interno que audita la organización en nombre de ella misma.

Auditor de segunda parte: (Inglés: *Second party auditor*). Auditor que audita una organización en nombre de otra. Por ejemplo, cuando una empresa audita a su proveedor *de outsourcing*, o cuando una administración pública ordena una auditoria de una empresa.

Auditor de tercera parte:(Inglés: *Third party auditor*). Auditor que audita una organización en

nombre de una tercera parte independiente que emite un certificado de cumplimiento.

Auditoría (inglés: *Audit*). Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y evaluarlas objetivamente para determinar el grado en el que se cumplen los criterios de auditoría.

Autenticación: (inglés: *Authentication*). Provisión de una garantía de que una característica afirmada por una entidad es correcta.

Autenticidad: (inglés: *Authenticity*). Propiedad de que una entidad es lo que afirma ser.

BS 7799: Norma británica de seguridad de la información, publicada por primera vez en 1995. En 1998, fue publicada la segunda parte. La parte primera era un conjunto de buenas prácticas para la gestión de la seguridad de la información -no certificable- y la parte segunda especificaba el sistema de gestión de seguridad de la información -certificable-. La parte primera es el origen de ISO 17799 e ISO 27002 y la parte segunda de ISO 27001:2013. Como tal estándar, ha sido derogado ya, por la aparición de éstos últimos.

BSI: *British Standards Institution*, la entidad de normalización del Reino Unido, responsable en su día de la publicación de la norma BS 7799, origen de ISO 27001:2013. Su función como entidad de normalización es comparable a la de AENOR en España.

Checklist: Lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y

profundidad y reduce los prejuicios del auditor y su carga de trabajo. Este tipo de listas también se pueden utilizar durante la implantación del SGSI para facilitar su desarrollo.

Compromiso de la Dirección: (Inglés: *Management commitment*). Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del **SGSI.** La versión de 2013 de ISO 27001:2013 lo engloba bajo la cláusula de Liderazgo.

Confidencialidad: (inglés: *Confidentiality*). Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Control correctivo: (Inglés: *Corrective control*). Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas relevantes. Supone que la amenaza ya se ha materializado pero que se corrige.

Control detectivo: (Inglés: Detective control). Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.

Control disuasorio: (Inglés: *Deterrent control*). Control que reduce la posibilidad de materialización de una amenaza, p.ej., por medio de avisos o de medidas que llevan al atacante a desistir de su intención.

Control preventivo:(Inglés: *Preventive control*). Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

Corrección:(Inglés: *Correction*). Acción para eliminar una no conformidad detectada. Si lo que se elimina es la causa de la no conformidad, véase acción correctiva.

Declaración de aplicabilidad: (Inglés: Statement of Applicability; SOA). Documento que enumera los controles aplicados por el SGSI de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- y su justificación, así como la justificación de las exclusiones de controles del Anexo A.9.2 Gestión de acceso de usuarios de ISO 27001:2013.

Desastre: (inglés: Disaster). Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

Directiva o directriz: (Inglés: *Guideline*). Una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

ENAC: Entidad Nacional de Acreditación. Es el organismo español de acreditación, auspiciado por la Administración, que acredita organismos que realizan actividades de evaluación de la

conformidad, sea cual sea el sector en que desarrollen su actividad. Además de laboratorios, entidades de inspección, etc., también acredita a las entidades de certificación, que son las que a su vez certificarán a las empresas en las diversas normas.

Entidad de acreditación: (Inglés: *Accreditation body*). Un organismo oficial que acredita a las entidades certificadoras como aptas para certificar según diversas normas. Suele haber una por país. Son ejemplos de entidades de acreditación: ENAC (España), UKAS (Reino Unido), EMA (México), OAA (Argentina), etc. En nuestra sección Normalización y Acreditación figuran todas las de países de habla hispana.

Entidad de certificación: (Inglés: *Certification body*). Una empresa u organismo acreditado por una entidad de acreditación para auditar y certificar según diversas normas (ISO 27001:2013, ISO 9001, ISO 14000, etc.) a empresas usuarias de sistemas de gestión.

Entidad de normalización: (Inglés: *Standards body*). Un organismo oficial que genera y publica normas. Suele haber una por país. Son ejemplos de entidades de normalización: AENOR (España), BSI (Reino Unido), DGN (México), IRAM (Argentina), etc. En nuestra sección Normalización y Acreditación figuran todas las de países de habla hispana.

Estimación de riesgos: (Inglés: *Risk evaluation*). Proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud son aceptable o tolerable.

Evaluación de riesgos: (Inglés: *Risk assessment*). Proceso global de identificación, análisis y

estimación de riesgos.

Gestión de incidentes de seguridad de la información: (Inglés: Information security incident management). Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

Gestión de riesgos: (Inglés: *Risk management*). Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

Identificación de riesgos: (Inglés: *Risk identification*). Proceso de encontrar, reconocer y describir riesgos.

IEC: International *Electrotechnical Commission*. Organización internacional que publica estándares relacionados con todo tipo de tecnologías eléctricas y electrónicas.

Impacto: (Inglés: *Impact*). El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc-.

Incidente de seguridad de la información: (Inglés: *Information security incident*). Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

ISC2: Information Systems Security Certification Consortium, Inc. Organización sin ánimo de lucro que gestiona diversas acreditaciones personales en el ámbito de la seguridad de la información.

ISMS: Information Security Management System. Véase: SGSI.

ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de entidades nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares (normas).

ISO 17799: Código de buenas prácticas en gestión de la seguridad de la información adoptado por ISO transcribiendo la primera parte de BS7799. Dio lugar a ISO 27002, por cambio de nomenclatura, el 1 de Julio de 2007. Ya no está en vigor.

ISO 19011: "Guidelines for auditing management systems". Norma con directrices para la auditoría de sistemas de gestión. Guía de utilidad para el desarrollo, ejecución y mejora del programa de auditoría interna de un SGSI.

ISO/IEC 27001:2013: Norma que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI). Primera publicación en 2005; segunda edición en 2013. Es la norma en base a la cual se certifican los SGSI a nivel mundial.

ISO/IEC 27002: Código de buenas prácticas en gestión de la seguridad de la información. Primera publicación en 2005; segunda edición en 2013. No es certificable.

ISO 9001: Norma que establece los requisitos para un sistema de gestión de la calidad.

ITIL: IT *Infrastructure Library*. Un marco de gestión de los servicios de tecnologías de la información.

ITSEC: Criterios de evaluación de la seguridad de la tecnología de información. Se trata de criterios unificados adoptados por Francia, Alemania, Holanda y el Reino Unido. También cuentan con el respaldo de la Comisión Europea (véase también TCSEC, el equivalente de EEUU).

JTC1: Joint Technical Committee. Comité técnico conjunto de ISO e IEC específico para las tecnologías de la información.

NIST: (ex NBS) Instituto Nacional de Normas y Tecnología, con sede en Washington, D.C.

No conformidad: (Inglés: *Nonconformity*). Incumplimiento de un requisito.

No repudio: Según [CCN-STIC-405:2006]: El no repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación. Según [OSI ISO-7498-2]: Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).

Objetivo: (inglés: Objetive). Declaración del resultado o fin que se desea lograr mediante la

implementación de procedimientos de control en una actividad determinada.

Parte interesada: (Inglés: *Interested party / Stakeholder*). Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

PDCA: Plan-Do-Check-Act. Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI). La actual versión de ISO 27001:2013 ya no lo menciona directamente, pero sus cláusulas pueden verse como alineadas con él.

Plan de continuidad del negocio: (Inglés: *Bussines Continuity Plan*). Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.

Plan de tratamiento de riesgos: (Inglés: *Risk treatment plan*). Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Política de escritorio despejado: (Inglés: *Clear desk policy*). La política de la empresa que indica a los empleados que deben dejar su área de trabajo libre de cualquier tipo de informaciones susceptibles de mal uso en su ausencia.

Proceso: (inglés: *Process*). Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.

Propietario del riesgo: (Inglés: *Risk owner*). Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.

Recursos de tratamiento de información (Inglés: *Information processing facilities*). Cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizadas para su alojamiento.

Residual *risk* Véase: Riesgo residual.

Riesgo (inglés*: Risk*). Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Riesgo residual (inglés: *Residual risk*). El riesgo que permanece tras el tratamiento del riesgo.

Sarbanes-Oxley: Ley de Reforma de la Contabilidad de Compañías Públicas y Protección de los Inversores aplicada en EEUU desde 2002. Crea un consejo de supervisión independiente para supervisar a los auditores de compañías públicas y le permite a este consejo establecer normas de contabilidad así como investigar y disciplinar a los contables. También obliga a los responsables de las empresas a garantizar la seguridad de la información financiera.

SC27: Subcomité 27 del JTC1 (Joint Technical Committee) de ISO e IEC. Se encarga del desarrollo de los estándares relacionados con técnicas de seguridad de la información.

Segregación de tareas: (Inglés: *Segregation of duties*). Reparto de tareas sensibles entre distintos empleados para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

Seguridad de la información: (Inglés: *Information security*). Preservación de la confidencialidad, integridad y disponibilidad de la información.

Selección de controles: (Inglés: *Control selection*). Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

SGSI: (inglés: ISMS). Véase: Sistema de Gestión de la Seguridad de la Información.

Sistema de Gestión de la Seguridad de la Información: (Inglés: *Information Security Management System*). Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

Tratamiento de riesgos: (Inglés: *Risk treatment*). Proceso de modificar el riesgo, mediante la implementación de controles.

Trazabilidad: (inglés: *Accountability*). Según [CESID: 1997]: Cualidad que permite que todas las

acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

UNE 71502: Norma española de ámbito local como versión adaptada de BS7799-2. Ya no está en vigor.

Vulnerabilidad: (inglés: *Vulnerability*). Debilidad de un activo o control que puede ser explotada por una o más amenazas.
((ISO), 2005)

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del Anexo A.9.2 Gestion de acceso de usuarios de ISO 27001:2013. (ISO/IEC 27000).

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000). Seguridad de la información

Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Trazabilidad. Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

Parte interesada: (*Stakeholder*) Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad. (MINISTERIO TIC , 2014)

1.6.3 MARCO LEGAL

LEY / RESOLUCIÓN CIRCULAR	TEMA
Ley 527 de 1999 Comercio Electrónico	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones"
Ley 599 DE 2000	Por la cual se expide el Código Penal. En esta se mantuvo la estructura del tipo penal de "violación ilícita de comunicaciones", se creó el bien jurídico de los derechos de autor y se incorporaron algunas conductas relacionadas indirectamente con el delito informático, tales como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Se tipificó el "Acceso abusivo a un sistema informático", así: "Art. 195. El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa."
Ley 962 de 2005	Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos. Prevé el incentivo del uso de medios tecnológicos

	integrados para disminuir los tiempos y costos de realización de los trámites por parte de los administrados.
Ley 1150 de 2007	Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos. Específicamente, se establece la posibilidad de que la administración pública expida actos administrativos y documentos y haga notificaciones por medios electrónicos, para lo cual prevé el desarrollo del Sistema Electrónico para la Contratación Pública, Seco.
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones
Ley 1341 de 2009	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la Información y las Comunicaciones TIC, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones
Resolución de la Comisión de Regulación de Comunicaciones	Sobre seguridad de las redes de los proveedores de redes y servicios de telecomunicaciones. Esta resolución modifica los artículos 22 y 23 de la Resolución CRT 1732 de 2007 y los artículos 1,8 y 2,4 de la Resolución CRT 1740 de 2007. Esta regulación establece la

2258 de 2009	obligación para los proveedores de redes y/o servicios de telecomunicaciones que ofrezcan acceso a Internet de implementar modelos de seguridad, de acuerdo con las características y necesidades propias de su red, que contribuyan a mejorar la seguridad de sus redes de acceso, de acuerdo con los marcos de seguridad definidos por la UIT, cumpliendo los principios de confidencialidad de datos, integridad de datos y disponibilidad de los elementos de red, la información, los servicios y las aplicaciones, así como medidas para autenticación, acceso y no repudio. Así mismo, establece obligaciones a cumplir por parte de los proveedores de redes y servicios de telecomunicaciones relacionadas con la inviolabilidad de las comunicaciones y la seguridad de l a información
Circular 052 de 2007 (Superintendencia Financiera de Colombia)	Fija los requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y Canales de distribución de productos y servicios para clientes y usuarios.

Tabla 2: Marco Legal

(Telecomunicaciones, 2011)

1.7 METODOLOGIA

En la presente investigación se pretende dar un enfoque más amplio en cuento a la implementación de los controles del sistema de seguridad de la información en la entidad toda vez que a pesar que se tienen avances por parte del departamento de informática no ha sido posible diagnosticar e implementar en su totalidad.

El sistema de gestión de la seguridad de la información es denominado un sistema trasversal, razón por la cual afecta a todas las dependencias dentro del mapa de procesos de la Superservicios que se anexa y que no todos los que hacen parte de la entidad conocen del sistema, sus alcances y por qué se debe implementar.

1.7.1 Tipo de Estudio:

El tipo de estudio utilizado en esta investigación es descriptivo según Sampiere indica en su libro metodología de la Investigación que: *"La Investigación descriptiva busca especificar propiedades, características y rasgos importantes de cualquier fenómeno que se analice. Describe tendencias de un grupo o población. El investigador debe ser capaz de definir, o al menos visualizar, que se medirá (que conceptos, variables, componentes, etc.) y sobre que 0 quienes se recolectaran los datos (personas, grupos, comunidades, objetos, animales, hechos, etc.)."* ***(Sampieri, 2006, pág. 102)***

Ahora bien, el análisis se realizó teniendo en cuenta la poca importancia que los funcionarios y contratistas le han dado al sistema de gestión de la seguridad de la información y adicionalmente el escaso avance que se ha tenido frente a la implementación de este.

Por otra parte, se debe concientizar a todo el personal de la importancia de dicha implementación, toda vez que generará conciencia y confianza en cuanto a la información que se maneja. La investigación se llevó a cabo partiendo de la base que la SSPD a lo largo del tiempo no cuenta con el apoyo suficiente de la alta dirección y se han ido encontrando falencias en cómo se está compartiendo y almacenado la información que se maneja, siendo esta el factor misional más importante. Detectándose de esta manera un alto riesgo que puede llevar a la entidad a que la información se pierda o pueda ser manipulada por terceros creando conflictos internos y externos, tales como que la información pueda ser usada mal intencionadamente.

El diagnóstico inicial se realizó a través de un trabajo de campo (encuesta) con el fin de saber cómo se encuentra actualmente el control de acceso en la entidad por parte de los funcionarios y contratistas de la entidad, con el fin de determinar y analizar el corregir todas las falencias encontradas; tomando como base la Norma ISO/IEC 27001: 2013 Anexo 9.

Este estudio será tomado como soporte para que la entidad comience un nuevo estudio basado en la situación actual de la entidad frente al sistema de seguridad que se está manejando porque a pesar que se cuenta con una política de calidad no se está cumpliendo o simplemente muchos no la conocen. Adicionalmente se pretende que se tomen medidas que se consideren pertinentes con la finalidad de encontrar las falencias y corregirla como paso inicial.

Teniendo en cuenta lo anterior, el diagnostico se realizó tomando como base los siguientes métodos de recolección de la información

- Observaciones
- Entrevista con el ingeniero encargado del proceso
- Documentos existentes en la entidad que se toman como base para realizar la implementación como lo son los diferentes modelos del ministerio de las telecomunicaciones
- Evaluación

La implementación del sistema de seguridad en la entidad se realizara por medio de etapas, teniendo en cuenta que el alcance del Modelo de Seguridad y Privacidad de la Información debe incluir todos los procesos de la entidad.

1.7.2 Etapas Previas:

Estado actual de la entidad: la entidad en este momento no cuenta con un sistema de seguridad de la información adecuado y acorde con la Norma ISO/IEC: 27001:2013, falta realizar el análisis de la información que se maneja en cada una de las áreas toda vez que se manejan temas específicos en cada una de ellas y los permisos de accesibilidad se deben llevar a cabo de acuerdo a sus funciones.

Identificar el nivel de madurez de la entidad frente a los sistemas de información:

Para esta etapa se realizó el diligenciamiento de una encuesta para determinar el grado de madurez con la que se cuenta actualmente en la entidad con lo relacionado al Anexo A.9.2 Gestion de

acceso de usuarios numeral 9.2.1 y 9.3.1de la Norma ISO/IEC/IEC 27001:2013.

Esta etapa se tiene clara frente al nivel organizacional, el inconveniente fundamental es que no se cuenta actualmente con el presupuesto adecuado para llevarlo a cabo. Además se considera como una falencia de alto grado la rotación de personal en el departamento de seguridad de la información ya que no permite la continuidad en el proceso y no sería conveniente tercer izar este proceso dentro de la entidad.

1.7.3 Etapa de Planificación:

En esta fase se pretende identificar que tan segura se encuentra la información tanto para usuarios internos como externos.

Se pretende identificar a través del control de acceso a la información

Se deben identificar las falencias que generan riesgos para mitigarlos de la manera más adecuada

Se deben identificar las necesidades de la entidad, expectativas de las partes interesadas.

Como también identificar riesgos y oportunidades, objetivos y planes para lograrlo.

Procedimientos establecidos

Los procedimientos asociados al Modelo deben ser implementados y utilizados dentro de las áreas de la Entidad, además deben ser aprobados por el Sistema de Gestión de Calidad. Dentro de los cuales se pueden encontrar y serán aplicados en cada capítulo posterior según sea el requerimiento.

- ✓ Procedimiento de capacitación y sensibilización del personal
- ✓ Procedimiento de ingreso y desvinculación del personal
- ✓ Procedimiento de identificación y clasificación de activos
- ✓ Procedimiento para ingreso seguro a los sistemas de información:
- ✓ Procedimiento de gestión de usuarios y contraseñas
- ✓ Procedimiento de mantenimiento de equipos

Otros aplicables:

Acciones para tratar riesgos y oportunidades de seguridad de la información.

Utilizar una metodología de gestión del riesgo enfocada a procesos, para este caso se sugiere utilizar la metodología del Departamento Administrativo de la Función Pública – DAFP, que contiene los siguientes pasos:

Identificación y valoración de riesgos de (Metodología, Reportes).

Tratamiento de riesgos (Selección de controles).

Toma de conciencia.

La Entidad debe definir un Plan de comunicación, sensibilización y capacitación que incluya la estrategia para que la seguridad de la información se convierta en cultura organizacional, al generar competencias y costumbres en todos aquellos que tienen que ver con la seguridad de la información en las entidades.

Este plan será ejecutado, con el aval de la alta dirección, a todas las áreas de la Entidad.

Para estructurar dicho plan puede utilizar la Guía para el plan de comunicación, sensibilización y capacitación.

Los resultados asociados a las metas en la Fase de Planificación deben ser revisados y aprobados por la alta Dirección.

1.8 DISEÑO METODOLOGICO

1.8.1 Diagnostico

Encuesta de seguridad: Gestion de Acceso

Aplicabilidad de las Políticas general de seguridad de la información para la superintendencia de servicios públicos.

1.8.2 Planear

Procedimientos de Seguridad y Privacidad de la Información.

Este documento contiene una plantilla que le ayudara a construir procedimientos de seguridad de la información.

Gestión del riesgo

file:///C:/Users/Escritorio/Downloads/Guia_Administracion_Del_Riesgo__DAFP.pdf

Este documento presenta una metodología para la gestión del riesgo al interior de las entidades del Estado en el marco del Programa de Gobierno en línea.

Controles de seguridad y Privacidad de la Información

Este documento presenta el conjunto de políticas que deben ser cumplidas por las entidades

Controles recomendados para que la entidad genere el documento de aplicabilidad de controles para el Sistema de Gestión de Seguridad de la Información.

Indicadores de gestión

1.8.3 Análisis

Mejora continúa

Este documento presenta 1.7.2 sepan cómo estructurar el desarrollo de fase de mejora continua del Modelo de Seguridad y Privacidad de la Información.

CAPITULO II

Analizar y realizar un diagnóstico de seguridad en el acceso de usuarios autorizados y no autorizados con los que se cuenta actualmente la Superintendencia de Servicios Públicos. – Norma ISO/IEC 27001:2013 Anexo A.9.2.1 Registro y cancelación de usuarios

La superintendencia de servicios públicos cuenta con el apoyo del Ministerio de tecnologías de la información y las comunicaciones – Min TIC a través de la dirección de estándares y arquitecturas de TI y la Subdirección de Seguridad y Privacidad de TI, dando cumplimiento a sus funciones; publica El Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia GEL: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión.

Según el organigrama de la entidad por ser el sistema de gestión de seguridad de la información un sistema trasversal como anteriormente se había dicho, hace parte de la oficina de informática, razón por la cual son los responsables directos de este proceso

Ilustración 5: Organigrama

Fuente: La Entidad

2.1 DIAGNOSTICO:

En la actualidad la Superservicios cuenta con un procedimiento para la *Gestión de Solicitudes de Servicios*, identificado con el código GT-P-003 dentro del Sistema Integrado de Gestión Mejora - SIGME, ubicado en el subproceso *Gestión y Operación de la Infraestructura Tecnológica* y perteneciente al proceso *Gestión Tecnologías de la Información*, en la cual las solicitudes relacionadas con la administración de usuarios (creación, modificación, activación y eliminación) a los diferentes aplicativos de la entidad, se tramitan a través del formato GT-F-004 *Administración de Usuarios*. Dicho procedimiento está documentado y publicado en el SIGME,

pero como todo proceso si no es automatizado es propenso a errores ya sea por fallas humanas intencionales o no intencionales. Además, el formato es diligenciado por los jefes de las diferentes áreas, cuando se producen ciertos eventos como son: la terminación de relación laboral de funcionarios y/o contratistas, el movimiento de las personas a otras áreas y el cual implica cambio de roles y por ende la activación a otros sistemas y servicios y la desactivación de accesos previamente otorgados.

Si se analiza con detenimiento, los eventos anteriormente descritos obedecen a efectos pero las causas no son abordadas de la menor manera.

Por lo cual, se sugiere que la mejor manera para controlar el acceso de los usuarios a los sistemas y aplicaciones, se debe producir cuando ocurren las novedades de personal, sean estas de funcionarios (Nomina de Personal) o contratistas (Contratos).

A continuación, se presenta el diagnóstico con respecto del acceso de los usuarios a los sistemas y aplicaciones, que deben ser considerados para poder automatizar dicho proceso de manera eficiente:

- Hay diferentes directorios activos para el acceso a aplicaciones: UNIX (LDAP del Sistema Único de Información- SUA, LDAP de aplicaciones Internals), Windows (Directorio Activo, Mesa de Ayuda, Bases de datos SQL Server, etc.).
- Se implementó el sistema Single Sign On, el cual centraliza la contraseña de usuarios de muchos aplicativos, pero no garantiza eficacia de administración de usuarios, debido a que no está implementada para todas las aplicaciones.

- Existen aplicativos legados con su propia autenticación.
- No existe control de usuarios creados en algunos aplicativos, deberían estar inactivos, pero siguen activos y acceden a la información de la SSPD, así se hayan implementado políticas que después de tres meses de inactividad, los usuarios sean inactivados automáticamente.
- No hay estándares para la identificación de usuarios.
- Diferentes tipos de codificación de caracteres (UTF8, UTF-16, ISO-8859, etc) en los sistemas y aplicativos, que dificultan el control de acceso a estos.
- El número de usuarios activos supera el número de licencias actuales, lo anterior obedece a que hay usuarios activos que deberían estar en estado inactivo porque ya no hacen parte de la entidad
- Hay diferentes administradores de aplicaciones y usuarios.
- El formato GT-F-004 *Administración de Usuarios* usado para la administración de usuarios, no garantiza que por medio de él se consignen todas las aplicaciones a las que acceden los usuarios

Para poder realizar un diagnóstico óptimo sobre el acceso a la información se deben tener en cuenta tres factores importantes dentro de la organización los cuales son: CONFIDENCIALIDAD, INTEGRIDAD, DISPONIBILIDAD, son los tres factores más importantes dentro de la seguridad de la información toda vez que si se encuentran alienados y se logran controlar, se establece que los datos se encuentran seguros y no tienen problema de vulnerabilidad. Entonces:

Para determinar la confidencialidad de los datos se implementó un sistema cifrado a través de algoritmos que permiten aplicar por medio de una única clave secreta acceso a varias aplicaciones

pero esta contraseña debe ser bastante robusta. Actualmente se usa en la entidad para el acceso al computador, base de datos y sistema de gestión documental.

Por otra parte, en cuanto a la integridad de los datos: hace referencia a la exactitud de los datos, que se encuentran completos y que no puedan ser modificados como por ejemplo estructura, fechas, resumen de información en el caso de la entidad.

La disponibilidad de los datos: hace referencia a que cuando se consultan, estos siempre se encuentren exequibles ya sea para ser consultados o analizados por el personal de la entidad, que se encuentren almacenados en un lugar seguro y se cuente con copias de seguridad (Back up).

Otro factor importante es establecer de manera apropiada la seguridad en las redes estableciendo mecanismos tales como los cortafuegos o firewall que ayudan a que personas inescrupulosas tengan accedo mal intencionado a la información.

Dicha protección debe hacerse de manera física como lógica toda vez los dispositivos también son susceptibles de ataques.

2.1.1 La protección de equipos

Los dispositivos también necesitan ser protegidos, se debe contar con un buen sistema operativo, que ayuden a fortalecer la seguridad del sistema operativo permitiendo que no lleguen ataques a las estaciones de trabajo y va estrechamente relacionada con la política de seguridad de la Superservicios. Queda por aclarar que la correcta implementación de la política de calidad,

facilita la administración de los sistemas operativos y por consiguiente todas las herramientas utilizadas en la seguridad de la información.

2.2 PLANEACIÓN

Realizando un análisis de fondo con respecto a las políticas de seguridad de la información se encuentra que no se cumple dentro de las diferentes áreas de la entidad, esta política fue dada bajo resolución y establece que:

"velar por mantener la integridad, confidencialidad y disponibilidad de la información que es recibida, procesada, generada o que reposa en la SUPERSERVICIOS"

Puede que los jefes de cada área la conozcan pero no se encuentran lo suficientemente comprometidos teniendo en cuenta que no se está cumpliendo con los requerimientos establecidos diligenciando el formato de desactivación de usuarios en la entidad para aquellas personas que ya no hacen parte de esa área o de la entidad a nivel general.

No se han dado cuenta de la importancia de mantener la información segura y más aun no se han dado a la tarea de analizar si llegará a pasar algo imprevisto con esta información como por ejemplo perdida de la misma. Se tiene el vago concepto que si esto llegara a suceder seria responsabilidad directa del área de informática.

Como falencia crítica no se encuentran documentos relacionados con el proceso de

seguridad de la información en la entidad, avances, riesgos, auditorias. Entre otros.

Únicamente en entrevista con el Ingeniero encargado del proceso se logra detectar que a pesar que se tienen claros cuales son los riesgos a los que se encuentra expuesta la entidad y cuáles son los controles que se deben implementar según la norma ISO para evitar estos, la alta gerencia no ha avalado dicha implementación. Verificando la base documental de la entidad se encuentra que a pesar que existen avances y se han tomado como guía los modelos de implementación del ministerio de telecomunicaciones el único avance que se ha tenido con respecto al personal encargado del SGSI es la capacitación tomada en dicho ministerio en el año 2016, avances para el año 2017 no han tenido.

2.3 ANALISIS

Tomando como análisis el año 2016, de las 25 áreas de la organización según el organigrama de la entidad se encontró lo siguiente:

Al finalizar el año solo se reportaron a la oficina de informática para la desactivación de usuarios 1020 incidencias entre los 754 funcionarios y 1230 contratistas, aún se desconoce el motivo por el cual no se reportaron las restantes, esto hace que el riesgo a la fuga de información genere un alto riesgo dentro de la entidad y la hace vulnerable a ataques mal intencionados por parte de terceros.

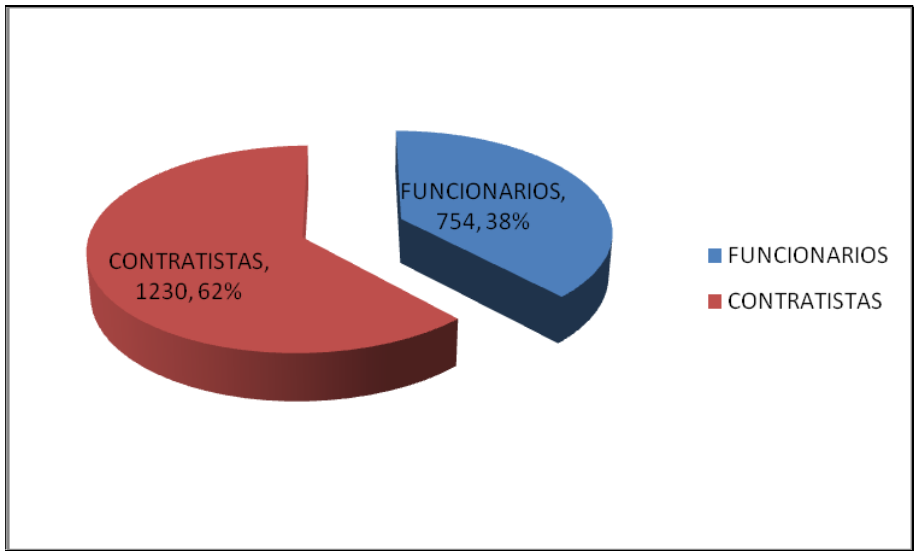

Ilustración 6: Total de personal laborando en la entidad al finalizar el año 2016

Fuente: El autor

Dentro del análisis establecido con la oficina de informática se concluyó:

1. el número de incidencias reportadas por parte de los jefes de área con respecto a los funcionarios de planta de la entidad no se reportaron porque al finalizar el año no tomaron receso o no fueron trasladados de área.

2. Con respecto a los contratistas, se presenta una situación diferente porque las incidencias reportadas por los encargados de cada área debieron haber reportado en su totalidad 1230 incidencias solicitado la desactivación de los usuarios a 31 de diciembre de 2016 toda vez que la entidad no compromete su presupuesto a vigencias futuras, es decir que todo el personal de prestación de servicios para este año debe terminar sus labores a más tardar el

ultimo día hábil del año.

3. Se demuestra que los responsables de cada área están incumpliendo con las políticas de seguridad de la información toda vez que como lo muestran los datos las incidencias reportadas no son acordes con lo que se espera en cuento al control de acceso de los usuarios de la entidad, no están diligenciando el registro que permite que la oficina de informática inhabilite los usuarios de manera efectiva generando un riesgo catalogado como alto ya que al momento de la finalización de los contratos ya el personal no tiene ningún vínculo con la entidad, esto en caso de las personas que se encuentran por prestación de servicios.

4. El proceso que se está utilizando no es el adecuado toda vez que la entidad debe implementar de manera inmediata un sistema automatizado que permita en tiempo real realizar el registro de cancelación de usuarios de manera inmediata sin que el jefe de área lo solicite sino simplemente crear un sistema que permita que cuando el contratista o funcionario comience sus labores registre la fecha de finalización o simplemente la novedad de hasta cuándo estará prestando sus servicios en la entidad según sea el caso.

Procedimiento utilizado actualmente en la Superservicios para la desactivación de Usuarios:

El procediendo para todos los jefes de área de la entidad consiste en diligenciar un formato en Excel que será enviado a través de Aranda.

Aranda Service Desk es una herramienta multiproyecto que permite gestionar diferentes procesos de negocio a través de una misma consola y dar soporte a diferentes tipos de casos como: Solicitudes, requerimientos de servicio, incidentes, problemas y cambios. Ofrece versatilidad para el registro y seguimiento de casos por parte del cliente, a través de la plataforma web de usuario final, permitiendo la autogestión de casos con la base de conocimientos o el registro de una nueva solicitud en la Mesa de servicio. http://arandasoft.com/aranda-service-desk/

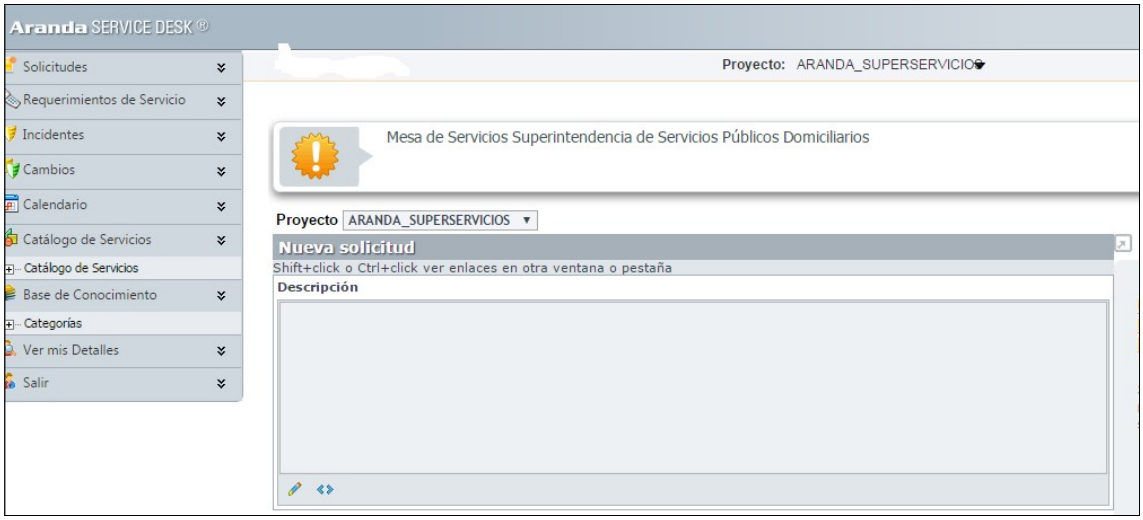

Ilustración 7: Aplicativo Aranda

Fuente: Entidad

A pesar que resulta ser una herramienta útil, quizás el error fundamental es que no se realiza la gestión de inactivación de usuarios por parte de la persona encargada o por error del personal encargado no se genera el requerimiento dentro del tiempo establecido ya que no es un sistema automatizado.

2.3.1 Riesgos

Matriz utilizada por la SSPD

MATRIZ DE CALIFICACIÓN, EVALUACION Y RESPUESTA A LOS RIESGOS

Probabilidad	Valor			
Alta	**3**	15 *Zona de riesgo moderado* Evitar el riesgo	30 *Zona de riesgo importante* Reducir el riesgo Evitar el riesgo Compartir o transferir	60 *Zona de riesgo inaceptable* Evitar el riesgo Reducir el riesgo Compartir o transferir
Media	**2**	10 *Zona de riesgo tolerable* Asumir el riesgo Reducir el riesgo	20 *Zona de riesgo moderado* Reducir el riesgo Evitar el riesgo Compartir o transferir	40 *Zona de riesgo importante* Reducir el riesgo Evitar el riesgo Compartir o transferir
Baja	**1**	5 *Zona de riesgo aceptable* Asumir el riesgo	10 *Zona de riesgo tolerable* Reducir el riesgo Compartir o transferir	20 *Zona de riesgo moderado* Reducir el riesgo Compartir o transferir
	Impacto	**Leve**	**Moderado**	**Catastrófica**
	Valor	**5**	**10**	**20**

Ilustración 8: Matriz de Riesgo

Fuente: Entidad

El principal riesgo que se encuentra es que si no es posible la inactivación de usuarios en tiempo real a las personas que tienen acceso a los diferentes aplicativos en la entidad se está genera un alto porcentaje de riesgo- que dentro de la norma se cataloga como ALTO.

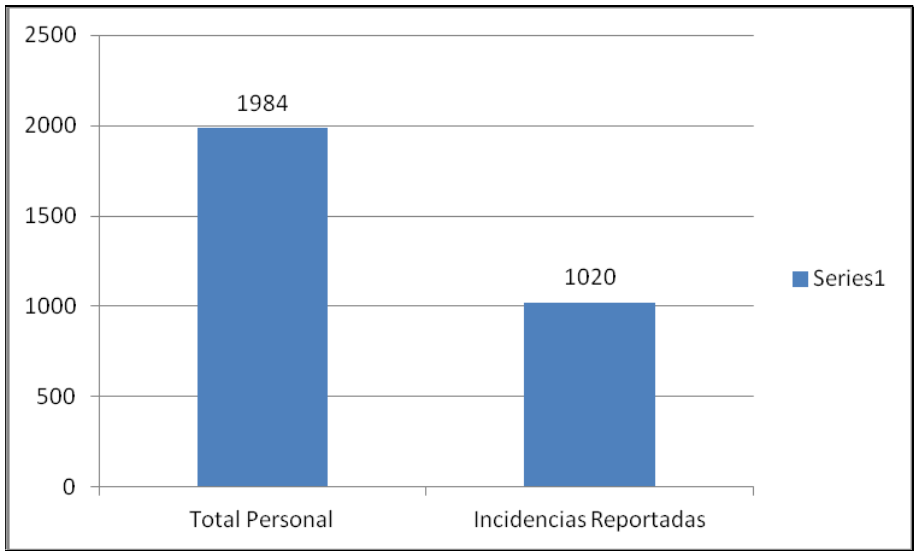

Ilustración 9: Nivel de Riesgo

Total de personal entidad a 2016 vs Incidencias de restricción a 2016

Fuente: el autor

Realizando un análisis sobre este hallazgo se logra identificar que del total del personal solo reportó el 51% para la desactivación de usuarios, el 49% restante quedaron activos.

Por otra parte, como la norma lo estipula la entidad deberá llevar una tabla de controles por área, en este caso el control estaría llamado como lo indica el anexo A.9 de la norma ISO/IEC 27001, en la cual se plasmaran los objetivos de control y se deberán estructurar como se indica a continuación:

Política general			
Núm.	Nombre	Seleccionado / Excepción	Descripción / Justificación
	Nombre	Control	
	...		

Tabla 3: Formato de Control

Fuente: http://www.mintic.gov.co /articles-5482_G8_Controles_Seguridad.pdf

- Donde cada campo se define así:
- Núm.: Este campo identifica cada uno de los controles correspondientes al Anexo A de la norma NTC: ISO/IEC 27001.
- Nombre: Este campo hace referencia al nombre del control que se debe aplicar para dar cumplimiento a la política definida.
- Control: Este campo describe el control que se debe implementar con el fin de dar cumplimiento a la política definida.
- Dominio: Este campo describe si el control aplica para uno o múltiples dominios.
- Seleccionado / Excepción: El listado de controles además debe ser utilizado para la generación de la declaración de aplicabilidad, donde cada uno de los controles es justificado tanto si se implementa como si se excluye de ser implementado, lo cual ayuda a que la entidad tenga documentado y de fácil acceso el inventario de controles.
- Descripción / Justificación: El listado de controles cuenta con la descripción de cada control en la tabla. Adicionalmente, es posible utilizarlo para la generación de la declaración de aplicabilidad, donde cada uno de los controles es justificado tanto si se

implementa como si se excluye de ser implementado.

Núm.	Nombre	Selección / Excepción	Descripción / Justificación
A.9	**Control de acceso**		
A.9.2	Gestión de acceso de usuarios		Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios
A.9.2.1	Registro y cancelación del registro de usuarios		Control: Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
A.9.2.2	Suministro de acceso de usuarios		Control: Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.
A.9.3	Responsabilidades de los usuarios		Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.
A.9.3.1	Uso de la información de autenticación secreta		Control: Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.

Tabla 4: Controles

Fuente: http://www.mintic.gov.co **/articles-5482_G8_Controles_Seguridad.pdf**

2.3.2 Hallazgos:

El objetivo es el de garantizar el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información y servicios.

Se deberían establecer procedimientos formales para controlar la asignación de los permisos de acceso a los sistemas y servicios de información.

Los procedimientos deberían cubrir todas las etapas del ciclo de vida del acceso de los usuarios, desde del registro inicial de los nuevos usuarios hasta su baja cuando ya no sea necesario su acceso a los sistemas y servicios de información.

Se debería prestar especial atención, si fuera oportuno, a la necesidad de controlar la asignación de permisos de acceso con privilegios que se salten y anulen la eficacia de los controles del sistema.

2.3.3 Actividades de control del riesgo

- Gestión de altas/bajas en el registro de usuarios: Debería existir un procedimiento formal de alta y baja de usuarios con objeto de habilitar la asignación de derechos de acceso.

- Retirada o adaptación de los derechos de acceso: Se deberían retirar los derechos de acceso

para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información a la finalización del empleo, contrato o acuerdo, o ser revisados en caso de cambio.

2.3.4 Métricas asociadas

Tiempo medio transcurrido entre la solicitud y la realización de peticiones de cambio de accesos y número de solicitudes de cambio de acceso cursadas en el mes anterior (con análisis de tendencias y comentarios acerca de cualquier pico / valle

2.3.5 Soluciones recomendadas

DBAudit: DB Audit es una completa solución out of the box de seguridad para bases de datos y auditoría para Oracle, Sybase, MySQL, DB2 y MS SQL Server.

Manage Engine: Solución web (free trial 30 days) que permite realizar las tareas más comunes, como las altas y bajas de usuarios y la aplicación de políticas de grupo, a través de un interfaz intuitivo y fácil de aprender. A través de sus informes detallados, ofrece visibilidad completa sobre todos los objetivos en el Directorio Activo.

Pangolin: Pangolin es una herramienta automática de pruebas de penetración de inyección SQL desarrollado por NOSEC. Su objetivo es detectar y aprovechar las vulnerabilidades de inyección SQL en aplicaciones web.

UserLock: Permite proteger el acceso a las redes de Windows®, impidiendo las conexiones

simultáneas, al dar la posibilidad de limitar las conexiones de los usuarios y proporcionando a los administradores el control remoto de las sesiones, de las funcionalidades de alerta, de informes y análisis sobre todas las conexiones/desconexiones efectuadas en sus redes.

CAPITULO III

Definir procesos apropiados para prevenir, atender, controlar y generar derechos de acceso para los sistemas y servicios con los que se cuenta actualmente en la Superservicios.

Mediante la adopción del Modelo de Seguridad y Privacidad por parte de las Entidades del Estado se busca contribuir al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de Seguridad Digital.

3.1 DIAGNOSTICO:

La entidad no cuenta con un procedimiento formal para la asignación, control y restricción de derechos de acceso y privilegios sobre sus recursos tecnológicos y aplicaciones.

Se toma como propósito fundamental la planeación de todos los factores que generen riesgo en cuanto al sistema de información que se ha implementado en la entidad, se deben prever todos los factores que impliquen riesgo, y se deben comenzar a controlar o atacar para encontrar una opción correctiva eficiente dentro de la entidad, este factor lo determina los permisos que cada jefe de área le asigna a sus subalternos dependiendo de sus roles y funciones dentro de la entidad.

Esta es la forma de asignación de permisos dentro de todas las áreas de la entidad, por medio del software Aranda y bajo un formato Signe se asignan las diferentes tareas para que el subalterno desarrolle a cabalidad sus funciones.

Dentro de la entidad el funcionario y contratista tendrá ingreso permitido a los siguientes aplicativos

1. Sistema de gestión documental ORFEO
2. Aranda: Mesa de ayuda
3. Sigme
4. Intranet
5. Correo electrónico institucional
6. Base de datos
7. Sistema único de información - SUI

se debe tomar como riesgo la siguiente secuencia: un evento externo o interno dentro de la entidad genera un registro de cierta información que se denomina dato, el cual es almacenado dentro de la base de base de dato que se almacena de manera automática dentro del repositorio y es denominada información oficial dentro de la Superservicios.

Dicha información que se encuentra almacenada es la que será vulnerable a riesgos.

En cuanto a los derechos de acceso la Superservicios podrá otorgar o denegar los permisos que considere pertinentes a los funcionarios o contratistas de la entidad según sean sus funciones,

determinado si los accesos a las aplicaciones son realmente fundamentales para el cumplimiento de sus funciones dentro de la entidad o en caso especial si se encuentran estipulados dentro de las funciones otorgadas que hagan parte esencial del desarrollo de estas. Las aplicaciones más utilizadas dentro de la entidad son: Correo electrónico institucional, sisgestion, Aranda, Orfeo y Sigme, entre otros.

Implementar el control A.9.2.2 *Suministro de acceso de usuarios* del Anexo A.9.2.2 ISO/IEC 27001:2013, cuyo objetivo es el de asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios con los que se cuenta actualmente en la Superservicios, de manera automatizada que permita ejercer un control efectivo apropiados sobre los procesos formales que se tienen el SIGME para el registro y cancelación de usuarios a los diferentes sistemas y servicios con que cuenta la entidad.

Para implementar lo anterior se requiere lo siguiente:

- Capturar las novedades de nómina (funcionarios) y las novedades de contratistas, para el control de activación, desactivación y modificación de roles de los usuarios que acceden a los diferentes sistemas y servicios.
- Para poder resolver lo anterior, la automatización propuesta debe ser capaz de comunicarse con las diferentes plataformas.
- Se deben poder realizar diferentes cruces de información de usuarios sin importar que sus llaves primarias difieran.
- Generar reportes de verificación a los diferentes líderes de procesos, que permitan confirmar la inactivación de usuarios, generados por la automatización

3.2 DATOS

Para cada una de las aplicaciones descritas anteriormente se tiene lo siguiente:

El sistema de gestión documental Orfeo, permite la creación de usuarios para todos los funcionarios y contratistas de la entidad, teniendo en cuenta que por medio de este sistema es que llegan todos los requerimientos internos y externos dentro de la entidad, permite de cierta manera la interacción entre áreas y es allí donde se almacena gran parte de la información que maneja la Superservicios.

Este sistema fue implementado en la entidad desde el año 2004 y ha tenido a lo largo del tiempo varias versiones que han permitido la comunicación de manera exitosa interna y externamente. Es un sistema robusto a nivel Colombia en cuanto a gestión documental se refiere. Actualmente muchas entidades estatales lo tiene implementado.

Es un sistema que permite

1. Crear usuarios
2. Modificar usuarios
3. Delimitar permisos de acceso
4. Inactivar usuarios
5. Crear grupos de usuarios

El sistema de gestión documental Orfeo maneja para cada área un código, dentro de ese código cada persona del área tiene habilitados permisos o TRD, solo los jefes de área podrán descargar los trámites de toda el área, lleva el tiempos de estado de trámite, permite generar respuestas de entrada y salida entre otros.

La falencia fundamental que se encuentra como en el capítulo anterior es que no se cuenta con un sistema automatizado que logre en tiempo real otorgar o denegar permisos según las responsabilidades que tengan los funcionarios y contratistas se debe comenzar la corrección de este riesgo dándoles a conocer a los jefes de área el formato que están obligados a diligenciar para que la oficina de informática pueda acceder al requerimiento que se pide y llevar un control del mismo.

Ahora bien, se logró determinar que no es falta de conocimiento de los jefes de área que no sepan cual es el proceso para otorgar o denegar permisos simplemente no lo hacen y a la oficina de informática le es complicado determinar qué clase de permisos requiere cada usuario dentro y fuera de la entidad.

La oficina de informática cuando es informada de esta clase de requerimientos implemento un formato de control de acceso y es a través de este que han podido hacer un seguimiento a esta clase de incidencias pero es poco eficaz.

3.3 ANALISIS DE RESULTADOS

Gestión de los derechos de acceso asignados a usuarios: Se debería de implantar un proceso formal de aprovisionamiento de accesos a los usuarios para asignar o revocar derechos de acceso a todos los tipos de usuarios y para todos los sistemas y servicios.

Gestión de los derechos de acceso con privilegios especiales: La asignación y uso de derechos de acceso con privilegios especiales debería ser restringido y controlado.

Revisión de los derechos de acceso de los usuarios: Los propietarios de los activos deberían revisar con regularidad los derechos de acceso de los usuarios.

INCIDENTES: es importante para comenzar un seguimiento apropiado al proceso para prevenir, atender, controlar y generar derechos de acceso para los sistemas y servicios con los que se cuenta actualmente en la Superservicios. Razón por la cual se debe conocer e implementar el modelo de gestión de incidentes. Este permitirá llevar un control acorde con las necesidades requeridas para las diferentes áreas de la entidad.

Ilustración 10: Modelo de Gestión de Incidentes

Fuente:http://www.mintic.gov.co/gestionti/615/articles-482_G21_Gestion_Incidentes.pdf

Se debe realizar un monitorio en cada una de las áreas al personal que en ellas intervienen y documentar por cada departamento los permisos que tienen cada uno toda vez que en el área de informática no se cuenta actualmente con esta información y es difícil identificar los permisos que cada uno de los miembros posee.

Esto a su vez permitirá llevar un control y seguimiento en cuanto a acceso y permisibilidad de la información en cada uno de los aplicativos con los que cuenta la entidad.

Este proceso debe ser documentado.

3.4 RIESGOS

IDENTIFICACIÓN DEL RIESGO

Riesgo Estratégico	Se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos y de políticas institucionales
Riesgos de Imagen	Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución
Riesgos Operativos	Comprenden riesgos provenientes del funcionamiento y operatividad de los procesos.
Riesgos Financieros	Manejo de los recursos económicos. Por ejemplo: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, etc
Riesgos de Cumplimientos	Capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.
Riegos de	Están relacionados con la capacidad tecnológica de la Entidad para satisfacer

Tecnología	sus necesidades actuales y futuras y el cumplimiento de la misión

Tabla 5: Identificación del Riesgo

Fuente: el autor

3.5 ANÁLISIS DEL RIESGO

Tabla de probabilidad

Nivel	Descriptor	Descripción	Frecuencia
1	Raro	El evento puede ocurrir solo en circunstancias excepcionales	No se ha presentado en los últimos 5 años
2	Improbable	El evento puede ocurrir en algún momento	Al menos de una vez en los últimos 5 años
3	Posible	El evento podría ocurrir en algún momento	Al menos de una vez en los últimos 2 años
4	Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias	Al menos de una vez en el último año
5	Casi cierto	Se espera que el evento ocurra en la mayoría de las circunstancia	Más de una vez al año

Tabla 6: Análisis Del Riesgo

Fuente: el autor

Tabla de impacto

Nivel	Descriptor	Descripción
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad
3	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad
4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos mínimos sobre la entidad
5	Catastrófico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos mínimos sobre la entidad

Tabla 7: Tabla de impacto

Fuente:

3.6 OPCIONES DE MANEJO DEL RIESGO

Opción	Descripción
Evitar	Tomar las medidas encaminadas a prevenir su materialización. Es siempre la primera alternativa a considerar, se logra cuando al interior de los procesos se generan cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas. **Por ejemplo:** El control de calidad, manejo de los insumos, mantenimiento,

	preventivo de los equipos, desarrollo tecnológico, etc
Reducir	Implica tomar medidas encaminadas a disminuir tanto la probabilidad, como el impacto. La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. **Por ejemplo:** A través de la optimización de los procedimientos y la implementación de controles.
Compartir o transferir	Reduce su efecto a través del traspaso de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido. **Por ejemplo:** La información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar, la tercerización
Asumir	Luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso, el gerente del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo.

Tabla 8: Opciones de Manejo del Riesgo

Fuente: el autor

3.7 MEJORA CONTINUA

RIESGO			
Fecha de Seguimiento y/o Actualización	05/12/2016	Versión:	1
Proceso/Subproceso:	GESTIÓN MEJORA CONTINUA	Objetivo del proceso/subproceso:	Gestionar el Sistema Integrado de Gestión y Mejora SIGME en el marco de la mejora continua, para facilitar la conformidad y eficacia de la gestión institucional.
Estado:	APROBADO	Responsable Actual:	

IDENTIFICACIÓN DEL RIESGO			
Actividad PCC:	Identificar lineamientos y controles para el Sistema Integrado de Gestión y mejora SIGME	Evento	Perdida de confidencialidad, integridad y disponibilidad de información de los procesos.

CAUSAS		
Descripción	Clasificación	Consecuencias
Ausencia de un Sistema de Gestión de Seguridad de la Información SGSI	INTERNA	Multas y sanciones; Cumplimiento de las funciones; Imagen institucional; Investigaciones disciplinarias.

Clasificación del Riesgo:	Estratégico

ANÁLISIS			
			Zona:
Probabilidad:	Nivel (de la probabilidad)	3	Extrema
	Descriptor (de la probabilidad)	POSIBLE	
Impacto:	Nivel (del impacto)	4	
	Descriptor (del impacto)	MAYOR	

VALORACIÓN CONTROLES	
Posee un instrumento para ejercer control:	SI

VALORACIONES CONTROL

Posee un instrumento para ejercer control	Descripción del(los) Instrumento(s)	Tipo de control	Ponderación Instrumentos de Control %	Se encuentra documentado en el SIGME el manejo del instrumento	En el tiempo que lleva el instrumento ha demostrado ser efectivo	Estan definidos los responsables de la ejecución y seguimiento del instrumento	La frecuencia de la ejecución del instrumento y seguimiento es adecuada	Calificación del Riesgo
SI	Definiciones de responsabilidades en los procedimientos, manuales e instructivos del SIGME.	PROBABILIDAD	100	SI	NO	SI	SI	70

Calificación del riesgo			
Probabilidad calificación	70.00 IMPROBABLE	Impacto Calificación	0 MAYOR
ZONA			
Alta			
Opciones de manejo:	Reducir	AC / AP / No:	AP-MC-006

Ilustración 11: Mejora continua

Fuente: el autor

Dicho acceso al sistema de información de la entidad está dado por los jefes de área quienes son las personas encargadas de determinar cuáles son los permisos que requieren los funcionarios o contratistas dependiendo del objeto de su contrato.

Se tiene un formato para determinar los permisos de los funcionarios y contratistas según las actividades que entren a desarrollar en la entidad. Pero contiene falencias múltiples teniendo en cuenta que en muchas oportunidades cuando cambian de área por rotación de

personal no diligencian a tiempo dicho formato y el funcionario adquiere cada vez más permisos accediendo a información que no le compete. No sea determinado en la entidad con exactitud quien es el responsable de esta falencia.

Se ha llegado a catalogar esta falencia como un riesgo de nivel alto, razón por la cual se ha establecido una conexión directa con el grupo de contratos para que a tres de un sistema sencillo se pueda identificar:

Cuando los contratistas están próximos a finalizar su contrato con la entidad y se genere una alerta que permita a tiempo realizar la desactivación de los recursos a los cuales tiene acceso en la entidad y se puedan deshabilitar en tiempo real los aplicativos a los cuales se le dio permisos incluyendo el correo electrónico institucional.

Cuando los funcionarios de la entidad salgan a vacaciones o a licencias remuneradas.

Los responsables de cada proceso deberán actualizar una vez al mes el sistema la información de las personas que tiene a su cargo para que se logre identificar si hay que restringir permisos

Con respecto a los prestadores de servicios públicos como tienen que realizar reporte de información mensual, trimestral y anualmente deberán realizar periódicamente o cuando lo consideren pertinente el cambio de contraseña.

Por otra parte, en cuanto a la consulta de la información por terceros la Superservicios en su paina web tendrá para su consulta los reportes de información actualizados, con la seguridad

que no se pueda modificar dicha información.

Determinar, controlar y restringir los derechos con los que cuentan los usuarios que tienen acceso a la información a la Superservicios, para ello se necesita:

Ir más allá de activar y desactivar usuarios relacionados con los diferentes sistemas y servicios, proponiendo nuevas maneras de controlar los accesos de usuarios a sistemas y servicios, según particularidades de la entidad.

Controlar posibles fallas a nivel de fuga de información.

Administrar de manera eficaz y eficiente los usuarios.

Proteger uno de sus activos más importantes, la información (Confidencialidad e integridad).

Automatizar los procesos de control de usuarios.

Realizar el control de incidentes mediante

CAPITULO IV

Verificar el cumplimiento de uso de información de autentificación secreta – Claves de acceso. Anexo A 9.3 Norma ISO/IEC 2013.

El objetivo principal es hacer que los usuarios sean responsables de la protección de la información para su identificación dentro y fuera de la entidad. Es importante dar a conocer a los funcionarios y contratistas que la cooperación de los usuarios autorizados es esencial para una seguridad efectiva.

Los usuarios deberían ser conscientes de sus responsabilidades en el mantenimiento de controles de acceso eficaces, en particular respecto al uso de contraseñas y seguridad en los equipos puestos a su disposición.

Se debería implantar una política para mantener mesas de escritorio y monitores libres de cualquier información con objeto de reducir el riesgo de accesos no autorizados o el deterioro de documentos, medios y recursos para el tratamiento de la información.

Se debe asegurar que se establecen las responsabilidades de seguridad y que son entendidas por el personal afectado. Una buena estrategia es definir y documentar claramente las responsabilidades relativas a seguridad de la información en las descripciones o perfiles de los puestos de trabajo.

Son imprescindibles las revisiones periódicas para incluir cualquier cambio. Comunique regularmente a los empleados los perfiles de sus puestos (p. ej., en la revisión anual de objetivos), para recordarles sus responsabilidades y recoger cualquier cambio.

Control del riesgo

Uso de información confidencial para la autenticación: Se deberá exigir a los usuarios el uso de las buenas prácticas de seguridad de la organización en el uso de información confidencial para la autenticación. Como por ejemplo que sus claves son únicos e intransferibles y que contengan números y letras. Adicionalmente que se cambien periódicamente como por ejemplo una vez al mes, también que se implemente un sistema que genere la alerta para que el usuario genere el cambio de manera inmediata.

Métricas asociadas

Porcentaje de descripciones de puesto de trabajo que incluyen responsabilidades en seguridad de la información

(a) totalmente documentadas y

(b) formalmente aceptadas.

Datos:

Para poder determinar y establecer que tan segura se encuentra la autenticidad de los usuarios en la entidad se realizó una encuesta con una población de 47 personas entre contratistas y funcionarios de la entidad. Preguntas cerradas de todas las áreas con el fin de poder dar a conocer la problemática actual de la entidad en cuanto al manejo de la información.

4.1 ENCUESTA

1. **Cuantas Contraseñas Maneja Actualmente. Por favor incluir las que utiliza actualmente en el trabajo y las que usa cuando usa internet**

OPCION	RESPUESTA	%
Una Contraseña (1)	**4**	10
tengo varias pero siempre utilizo la misma (2)	**4**	10
Tengo Dos Diferentes (3)	**8**	21
Tengo Tres Diferentes (4)	**7**	18
Tengo Cuatro O Mas (5)	**15**	38
No Poseo Contraseñas (6)	**1**	3

Tabla 9 : Respuesta de la pregunta 1

Fuente: Autor

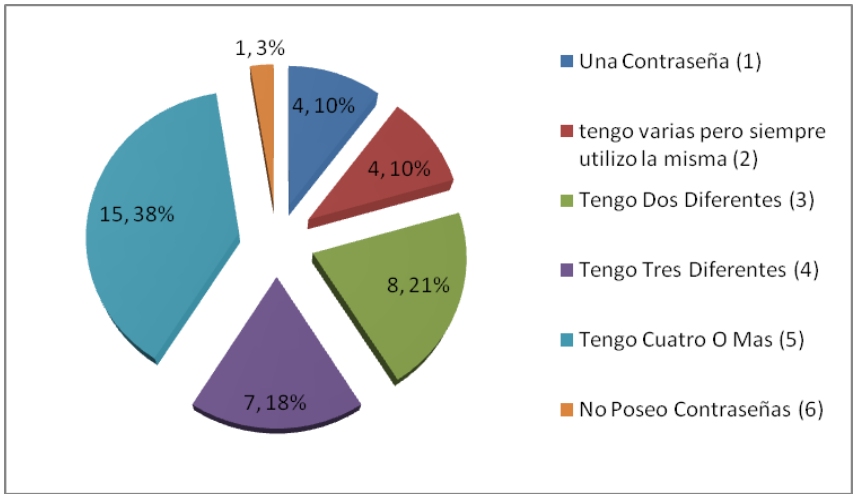

Ilustración 12: Grafica pregunta 1

Fuente: Autor

2. A Que Tipo De Información Accede Con Las Contraseñas

OPCION	RESPUESTA	%
Laboral Y Confidencial (1)	**15**	**32**
Personal Y Confidencial (2)	**9**	**19**
Todas Las Anteriores (3)	**23**	**49**

Tabla 10: Respuesta de la pregunta 2

Fuente: Autor

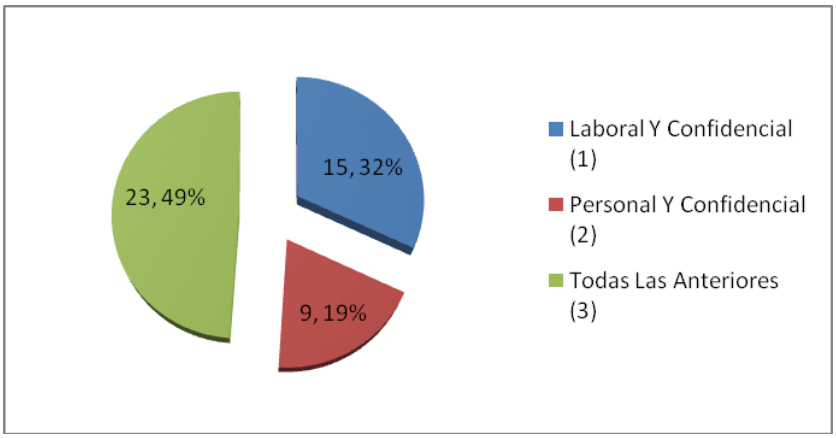

Ilustración 13: Grafica pregunta 2

Fuente: Autor

3. Que Criterios Utiliza Para Crear Las Contraseñas

OPCION	RESPUESTA	%
Utiliza Palabras Familiares (1)	**3**	7
Digita Fechas Especiales (2)	**1**	2
Utiliza Números Y Letras A La Vez (3)	**39**	83
Solo Dígitos (4)	**3**	6
Solo Letras (5)	**0**	0
Se La Asignan (6)	1	2

Tabla 11: Respuesta de la pregunta 3

Fuente: Autor

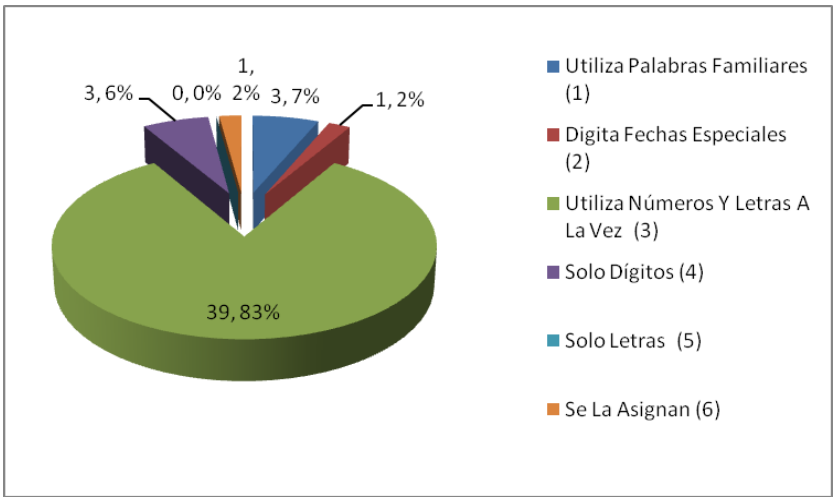

Ilustración 14: Grafica pregunta 3

Fuente: Autor

4. Olvida Fácilmente Sus Contraseñas

OPCION	RESPUESTA	%
SI (Y)	16	34
NO(N)	31	66

Tabla 12: Respuesta de la pregunta 4

Fuente: Autor

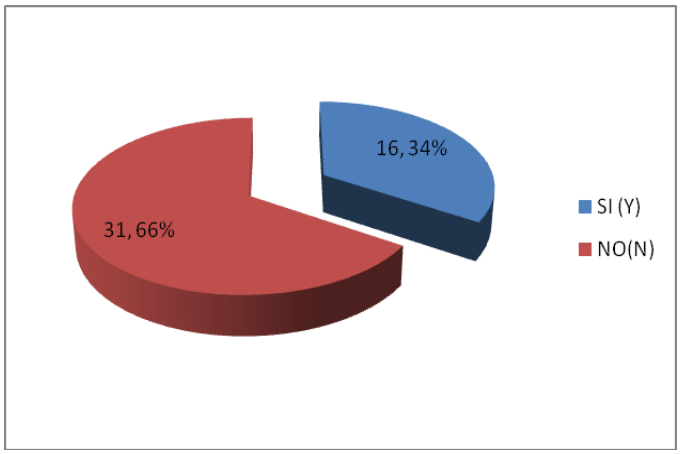

Ilustración 15: Grafica pregunta 4

Fuente: Autor

5. Escribe sus contraseñas en algún lugar

OPCION	RESPUESTA	%
SI (Y)	**13**	28
NO(N)	**34**	72

Tabla 13: Respuesta de la pregunta 5
Fuente: Autor

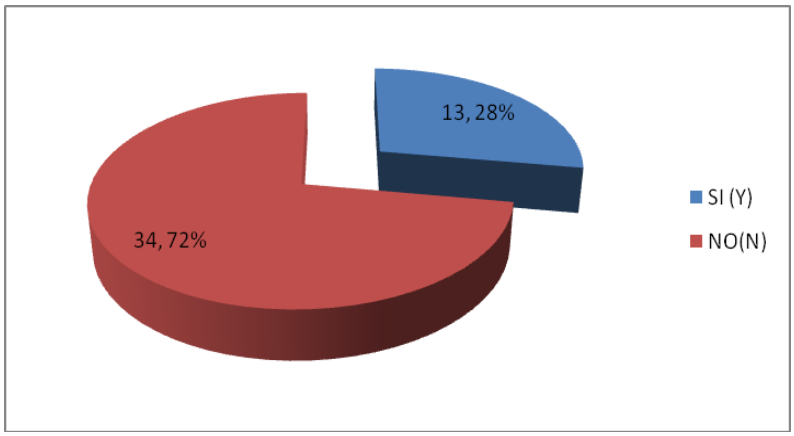

Ilustración 16: Grafica pregunta 5

Fuente: Autor

6. Donde Almacena Sus Contraseñas

OPCION	RESPUESTA	%
En Un Archivo De Texto (1)	**4**	8
En Una Libreta Personal (2)	**6**	13
Las Memorizo (3)	**22**	47
Mi Respuesta Anterior Fue No (4)	**15**	32

Tabla 14: Respuesta de la pregunta 6

Fuente: Autor

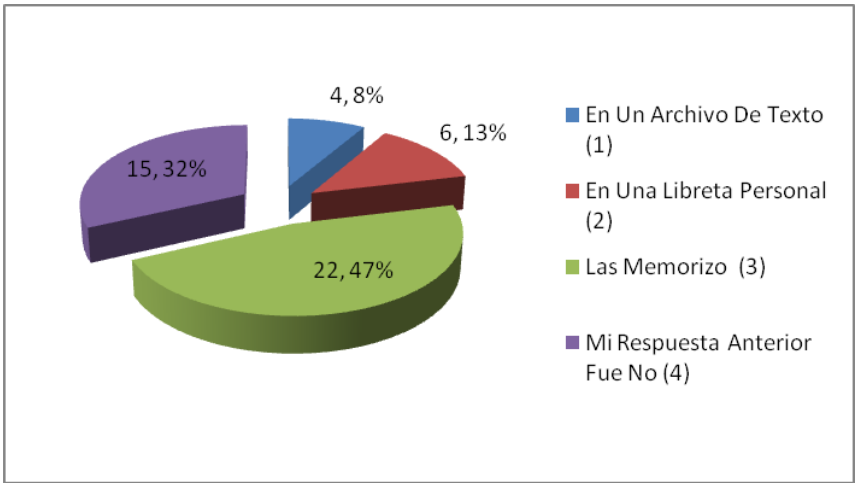

Ilustración 17: Grafica pregunta 6

Fuente: Autor

7. Cada Cuanto Tiempo Cambia Sus Contraseñas

OPCION	RESPUESTA	%
Cada Tres Meses (1)	**9**	19
Cada Seis Meses (2)	**10**	21
Cada Año (3)	**10**	21
Nunca (4)	**18**	39

Tabla 15: Respuesta de la pregunta 7

Fuente: Autor

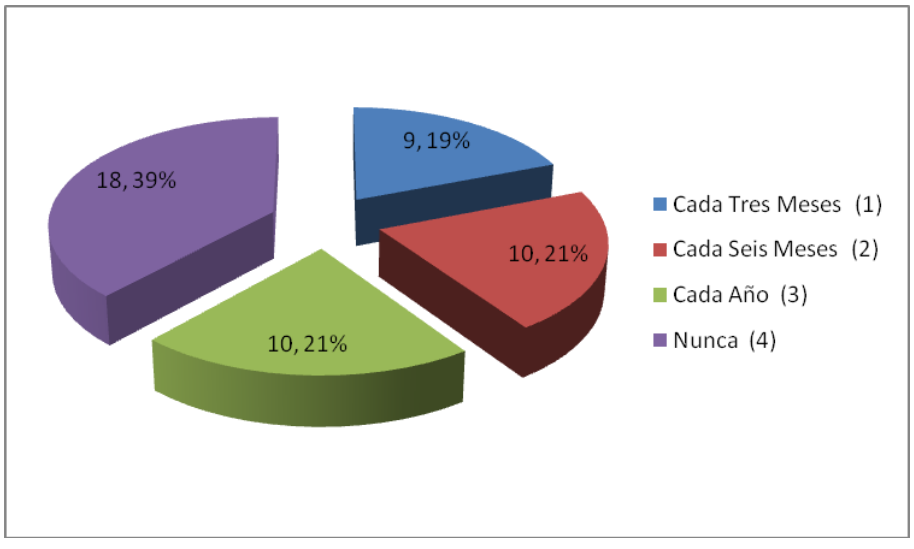

Ilustración 18: Grafica pregunta 7

Fuente: Autor

8. Quien le Asigna sus contraseñas

OPCION	RESPUESTA	%
La Entidad (1)	**5**	11
Las Creo Yo Mismo (2)	**42**	89

Tabla 16: Respuesta de la pregunta 8

Fuente: Autor

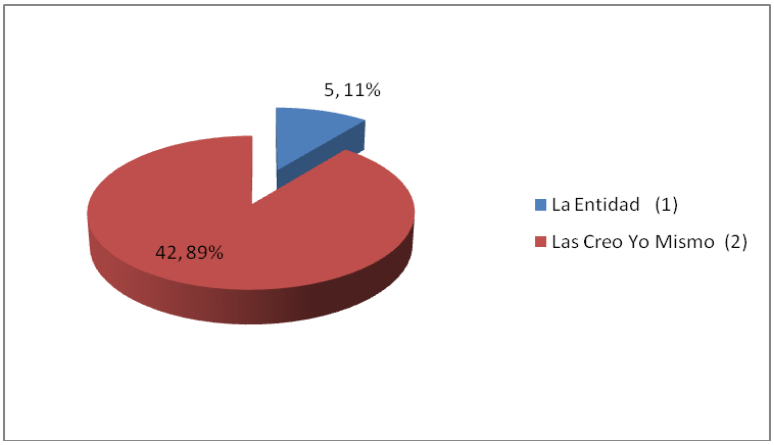

Ilustración 19: Grafica pregunta 8

Fuente: Autor

9. Comparte Contraseñas

OPCION	RESPUESTA	%
Algunas (1)	**14**	30
Todas (2)	**1**	2
No Las Comparto (3)	**32**	68

Tabla 17: Respuesta de la pregunta 9

Fuente: Autor

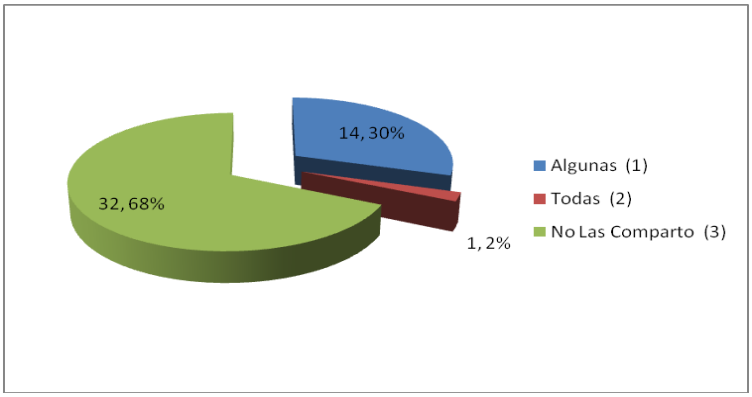

Ilustración 20: Grafica pregunta 9

Fuente: Autor

10. Existe alguna política o procedimiento impartido por la entidad para el manejo de las contraseñas

OPCION	RESPUESTA	%
SI (Y)	**23**	49
NO(N)	**24**	51

Tabla 18: Respuesta de la pregunta 10

Fuente: Autor

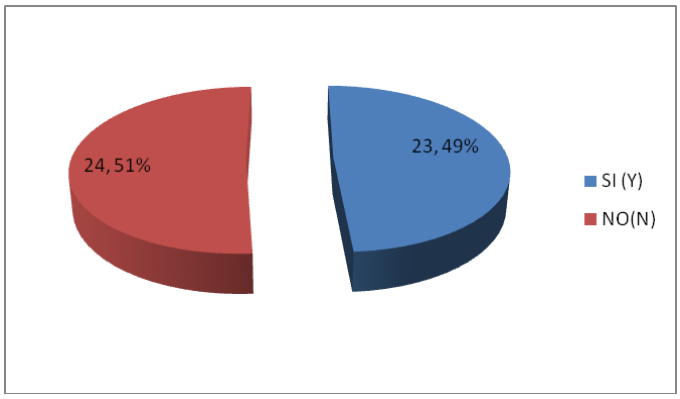

Ilustración 21: Grafica pregunta 10

Fuente: Autor

11. Numero de caracteres que utiliza para las contraseñas

OPCION	RESPUESTA	%
ENTRE 1 Y3 (1)	**11**	23
ENTRE 4 Y 6 (2)	**1**	2
MAS DE 6 (3)	**35**	75

Tabla 19: Respuesta de la pregunta 11

Fuente: Autor

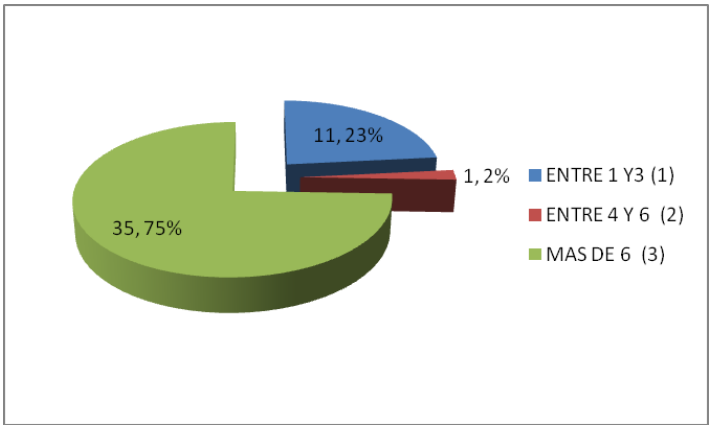

Ilustración 22: Grafica Pregunta 11

Fuente: Autor

12. tiene cuidado al digitar las contraseñas en presencia de otras personas

OPCION	RESPUESTA	%
Si, Algunas Veces (1)	**20**	43
Si , Siempre (2)	**23**	49
No Me Preocupa En Lo Absoluto (3)	**4**	8

Tabla 20: Respuesta de la pregunta 12 de la encuesta

Fuente: Autor

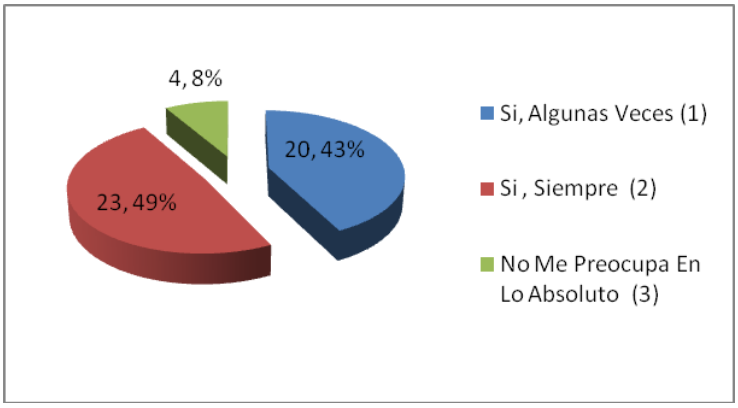

Ilustración 23: Grafica pregunta 12

Autor: Fuente

13. bloquea su equipo o cierra sesión cuando no está usando su computador

OPCION	RESPUESTA	%
Siempre (1)	**26**	**55**

A Veces (2)	**4**	**9**
Nunca (3)	**17**	

Tabla 21: Respuesta de la pregunta 13 de la encuesta

Autor: Fuente

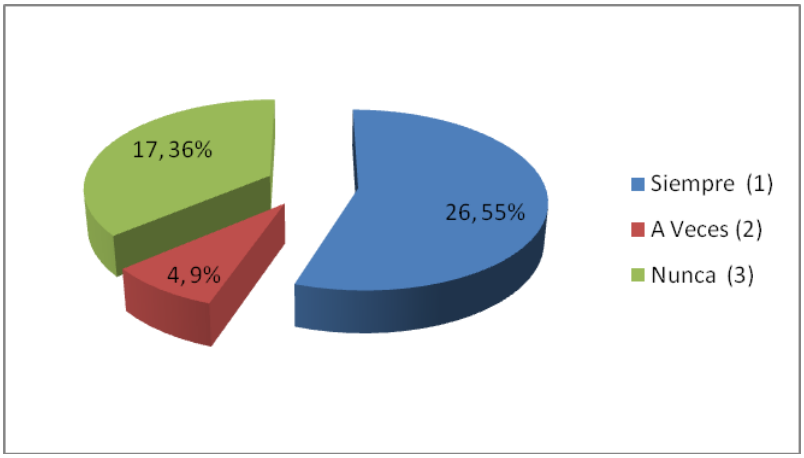

Ilustración 24: Grafica pregunta 13

Autor: Fuente

14. Solicita o cambia la contraseña cuando alguien la conoce

OPCION	RESPUESTA	%
SI (Y)	**36**	**77**
NO(N)	**11**	**23**

Tabla 22: Respuesta de la pregunta 14 de la encuesta

Autor: Fuente

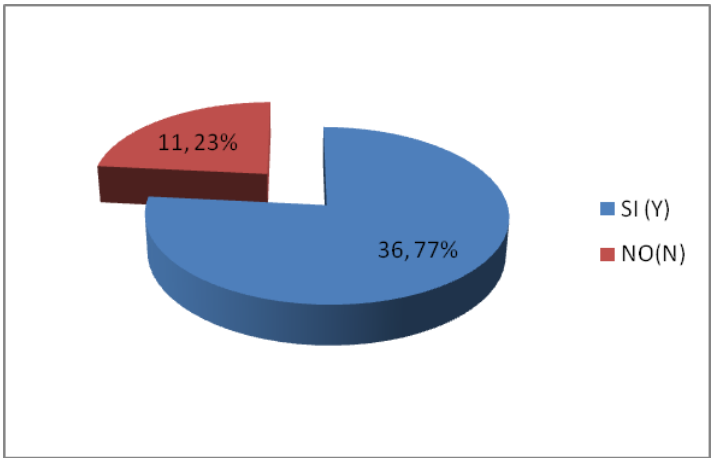

Ilustración 25: Grafica pregunta 14

Autor: Fuente

Soluciones recomendadas

KEEPASS: Es una aplicación para la gestión de contraseñas que sirve de ayuda para gestionar las contraseñas de un modo seguro. Puedes almacenar todas las contraseñas en una única base de datos, la cual permanece accesible mediante una única clave maestra o fichero. Por tanto, sólo se tiene que recordar una única contraseña o seleccionar el fichero clave para acceder a la base de datos cifrada mediante algoritmo robusto (AES y Twofish).

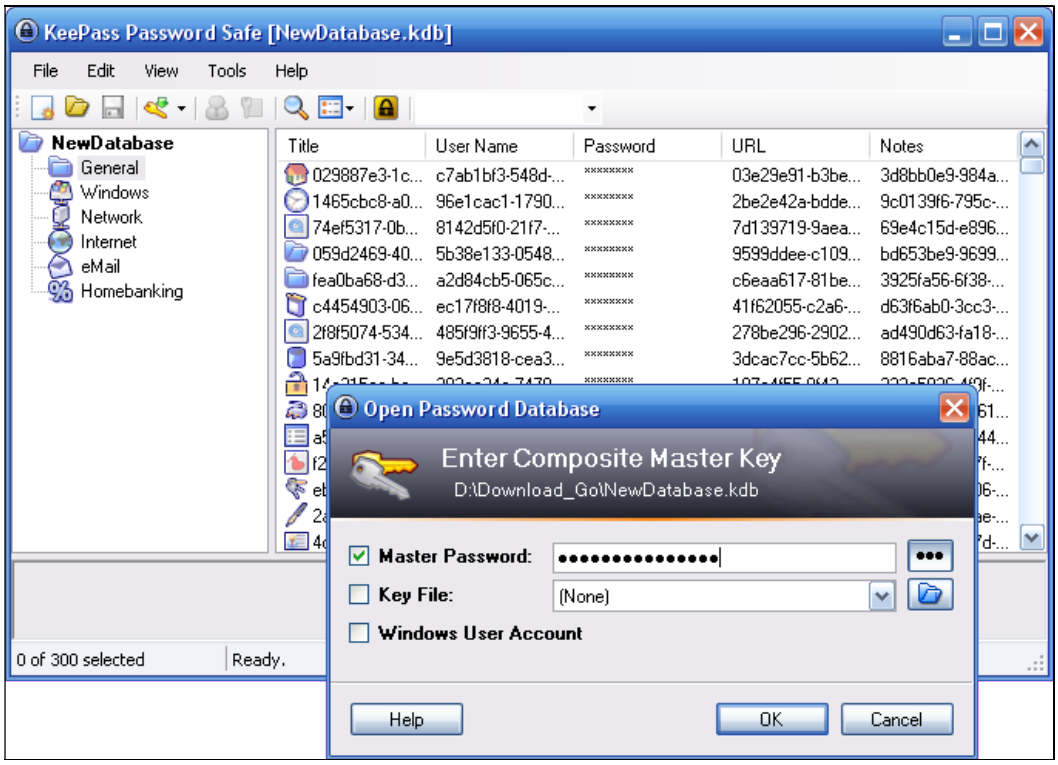

Ilustración 26: Aplicación Keepass

Fuente: Entidad

CONCLUSIONES

- Se realizó el análisis detallado de cada una de las fallas encontradas en seguridad en cuanto a lo que la supeservicios tiene implementado como control de acceso, dicho análisis determino establecer que no se cuenta con un modelo de seguridad óptimo y apropiado en la entidad, razón por la cual se está realizando un proyecto en el área de sistemas que se presentara a la alta dirección de la entidad (Despacho) para que se asignen los recursos pertinentes para poder comenzar su implementación. Dentro del proyecto se pretende atacar tres factores importantes tales como el reporte de incidencias de manera automática por parte de cada área haciendo un uso eficiente de la herramienta Aranda contando con dos únicas personas de esta área en el manejo de estas incidencias, de esta manera se podrán solventar y llevar un mejor control del procedimiento de desactivación de usuarios dentro de la entidad.

- Se determinó que no se cuenta actualmente con registros que permitan identificar en cada una de las áreas de la superservicios a que debe tener acceso el personal que labora según la labor que desempeña. Teniendo en cuenta esto, se debe implementar de manera inmediata por parte de la oficina de informática un procedimiento que permita dar acceso a estos profesionales según el perfil que tengan, esto permitirá llevar un control de habilitar y restringir los permisos a cada una de las herramientas con las que se cuentan dentro de la entidad toda con los que debe contar según la labor a desempeñar. Razón por la cual, por ser un procedimiento netamente informático, este departamento deberá tener la responsabilidad directa de controlar y restringir los accesos a los usuarios y de ser así, este procedimiento deberá ser revisado periódicamente para mantenerlo bajo control. Ya identificados los riesgos de no tener un control sobre la accesibilidad a las diferentes aplicaciones en la entidad se debe mejorar el procedimiento actualmente utilizado e implementarlo de forma detallada tomando como base los manuales que brinda el ministerio de tecnologías de la información.

- Según el estudio realizado en cuanto al uso de las contraseñas, se determinó que los funcionarios y contratistas que laboran actualmente en la entidad manejan distintas contraseñas poco seguras en los diferentes aplicativos que se manejan en la entidad, por esta razón dentro del proyecto se recomienda hacer uso de un software (KEEPASS) que le permita al usuario utilizar una única clave, la cual será administrado y controlado directamente por el área de informática.

- La propuesta de implementación de un mejor sistema de seguridad de la información, actualmente se encuentra en revisión por parte de la oficina de informática de la entidad para que posteriormente sea enviada al despacho del señor superintendente para su aprobación, porque se requiere de asignación de recursos para llevar a cabo las diferentes mejoras propuestas.

- Se debe reconocer que las diferentes entidades gubernamentales quieren estar a la vanguardia en cuanto a los diferentes sistemas de gestión toda vez que desde el año 2014 a través del Ministerio de las Telecomunicaciones (TIC) han estado capacitando y suministrando guías que

permitan a las entidades gubernamentales realizar de una manera más sencilla la implementación de un sistema de seguridad de la información.

- Gracias a las diferentes guías de implementación del sistema de seguridad de la información suministradas la Superservicios desde el año 2014 ha estado evaluando los recursos con los que cuenta para la realizar la implementación del sistema, la etapa del diagnóstico ya se encuentra ejecutada y de ser aprobado por parte de la alta dirección, se procederá con la implementación.

- Por otra parte, tomando como base la tabla de resultados del Diagnóstico de la implementación del sistema de seguridad de la información se encuentra que la entidad tiene falencias en cuento al manejo y control de la información y se cataloga como Riesgo Alto, el no tenerla bajo control y bajo la inspección que se requiere.

- También se debe tener en cuenta que la entidad requiere con urgencia dicha implementación para poder hacerle seguimiento y control a cada una de las falencias encontradas y descritas en la tabla No. 21, pero el problema fundamental que se encuentra en el área de informática es el presupuesto y el alto grado de rotación de personal, tomado como consecuencia que cada nueva administración pretende cambiar lo adelantado el año anterior, entonces el procedimiento en lugar de avanzar sufre un retroceso y se vuelve a tomar el proyecto de cero.

RECOMENDACIONES

Garantizar su Misión y Alcanzar su visión. El diseño de un Sistema de Gestión de Seguridad de la Información basado en la Norma ISO/IEC/IEC 27001:2013, proveerá los mecanismo adecuados para poder garantizar la protección y aseguramiento de su información, lo cual es fundamental para la debida y segura gestión administrativa, financiera, operativa y técnica de la entidad necesaria para poder garantizar su Misión y alcanzar su Visión.

Mejorar la Imagen de la entidad. Un Sistema de Gestión de Seguridad de la Información le provee a la entidad una metodología para la gestión de riesgos de seguridad de la información, lo cual mejora su imagen antes sus partes interesadas ya que genera confianza debido a que demuestra que la entidad identifica, clasifica, valora y trata de manera adecuada sus riesgos de seguridad.

Disminuir costos. Un Sistema de Gestión de Seguridad de la Información puede generar un impacto positivo en las finanzas de la entidad, ya que en la medida de que los colaboradores tengan una conciencia clara de cuál es la información que se debe proteger y gestionen adecuadamente sus riesgos, se puede evitar inversiones innecesarias en seguridad y tecnología.

Cumplimiento normativo. Sistema de Gestión de Seguridad de la Información permite determinar el estado real de la seguridad de la información de la entidad, conocer las posibles amenazas que la puedan afectar y establecer las acciones efectivas para mitigarlas, lo cual, indique una adecuada gestión de riesgos que garantizar la debida protección de su información y la

privacidad de los datos personales de sus clientes, lo cual, ayuda al cumplimiento de la normatividad vigente relacionada con seguridad de la información.

GLOSARIO

Activo de Información: Es todo aquello que las entidades consideran importante o de alta validez para la misma ya que puede contener importante información como lo puede ser Bases de Datos con usuarios, contraseñas, números de cuentas, etc.

Seria critico que a una entidad que maneja alta información confidencial, los intrusos pudieran acceder a ella afectando así la confidencialidad, la disponibilidad y la integridad de dicha información por eso algunas de tantas entidades adoptan un plan de seguridad para los activos de información y así no tener la desgracia de que los datos se fuguen, se modifiquen o se pierdan.
En general es toda la información que la entidad posee dentro de un activo informático tales como servidores, switch, etc.

Backup: Se refiere a la copia y archivo de datos de la computadora de modo que se puede utilizar para restaurar la información original después de una eventual pérdida de datos. La forma verbal es hacer copias de seguridad en dos palabras, mientras que el nombre es copia de seguridad.

Centro de Cómputo: Definición de centro de cómputo. Un centro de cómputo, centro de procesamiento de datos, centro de datos o data center es una entidad, oficina o departamento que se encarga del procesamiento de datos e información de forma sistematizada.

Confidencialidad: Es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información. La confidencialidad ha

sido definida por la Organización Internacional de Estandarización es como garantizar que la información es accesible sólo para aquellos autorizados a tener acceso, y es una de las piedras angulares de la seguridad de la información. La confidencialidad es uno de los objetivos de diseño de muchos criptosistemas, hecha posible en la práctica gracias a las técnicas de criptografía moderna.

Contraseña: o clave es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña debe mantenerse en secreto ante aquellos a quien no se le permite el acceso. A aquellos que desean acceder a la información se les solicita una clave; si conocen o no conocen la contraseña, se concede o se niega el acceso a la información según sea el caso

Control de Acceso: Un sistema de control de acceso es un sistema electrónico que restringe o permite el acceso de un usuario a un área específica validando la identificación por medio de diferentes tipos de lectura clave por teclado, tags de proximidad o biometría y a su vez controlando el recurso.

Correo Electrónico: El correo electrónico también conocido como e-mail, un término inglés derivado de electrónico mail es un servicio que permite el intercambio de mensajes a través de sistemas de comunicación electrónicos.

Descopilar: Un decompilador del inglés "descompilar", a veces castellanizado descompilador) es un programa de ordenador que realiza la operación inversa a un compilador. Esto es, traducir código o información de bajo nivel de abstracción sólo diseñado para ser leído por

un ordenador, máquina a un lenguaje o medio de mayor nivel de abstracción usualmente diseñado para ser leído por un humano, cualquier lenguaje de programación de alto nivel.

Desarrollo: Desarrollo significa crecimiento, progreso, evolución, mejoría. Como tal, designa la acción y efecto de desarrollar o desarrollarse. El concepto de desarrollo puede hacer referencia a una tarea, una persona, un país o cualquier otra cosa. En este sentido, podemos hablar de desarrollo cuando nos referimos a la ejecución de una tarea o la realización de una idea.

Disponibilidad: Se denomina disponibilidad a la posibilidad de una cosa o persona de estar presente cuando se la necesita. La disponibilidad remite a esta presencia funcional que hace posible dar respuestas, resolver problemas, o meramente proporcionar una ayuda limitada.

Dispositivo: Mecanismo, aparato o máquina que está preparado para una acción prevista.

Documento: Un documento es un testimonio material de un hecho o acto realizado en funciones por instituciones o personas físicas, jurídicas, públicas o privadas, registrado en una unidad de información en cualquier tipo de soporte (papel, cintas, discos magnéticos, fotografías, etc.) en lengua natural o convencional.

Documento Público: Un documento o instrumento público es aquel documento expedido o autorizado por un funcionario público o fedatario público competente y que da fe de su contenido por sí mismo. En general, son documentos públicos aquellos emitidos por funcionarios públicos en ejercicio de sus funciones. Documento expedido o autorizado por funcionario público competente con las solemnidades requeridas por la ley.

Hardware: La palabra hardware en informática se refiere a las partes físicas tangibles de un sistema informático; sus componentes eléctricos, electrónicos, electromecánicos y mecánicos.1 Cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado componen el hardware; contrariamente, el soporte lógico e intangible es el llamado software.

Ingeniera Inversa: Es el proceso de descubrir los principios tecnológicos de un objeto, herramienta, dispositivo o sistema, mediante el razonamiento abductivo haciendo conjeturas de su estructura, función y operación.

Información Sensible: Información sensible es el nombre que recibe la información personal privada de un individuo, por ejemplo ciertos datos personales y bancarios, contraseñas de correo electrónico e incluso el domicilio en algunos casos.

Insumos: El insumo es todo aquello disponible para el uso y el desarrollo de la vida humana, desde lo que encontramos en la naturaleza, hasta lo que creamos nosotros mismos, es decir, la materia prima de una cosa.

Integridad: Se traduce como honradez, honestidad, respeto por los demás, corrección, responsabilidad, control emocional, respeto por sí mismo, puntualidad, lealtad, pulcritud, disciplina, congruencia y firmeza en sus acciones. En general es alguien en quien se puede confiar. Integridad es retomar el camino de nuestra verdad, hacer lo correcto por las razones correctas del modo correcto. Se relaciona al derecho de no ser objeto de vulneraciones en la persona física, como lesiones, tortura o muerte.

Material no autorizado: Es de aclarar que el traslado del material a los Centros de Aprovechamiento se convierten desde allí en responsabilidad del operador del Centro de transferencia. (En estas zonas solo se acopia material que podrá aprovechar el Centro de Aprovechamiento de RCD que servirán para la elaboración de materiales de construcción). En ningún caso este podrá realizar labores de transformación.

Material multimedia: Los materiales multimedia son aquellos que permiten integrar de forma coherente diferentes códigos de información: texto, imagen, animación y sonido. Entre los materiales multimedia más utilizados en educación se encuentra el diaporama o presentación y el video.

Plan de contingencia: Un plan de contingencia es un conjunto de procedimientos alternativos a la operatividad normal de cada institución. Su finalidad es la de permitir el funcionamiento de esta, aun cuando alguna de sus funciones deje de hacerlo por culpa de algún incidente tanto interno como ajeno a la organización.

Red LAN: LAN son las siglas de Local Area Network, Red de área local. Una LAN es una red que conecta los ordenadores en un área relativamente pequeña y predeterminada (como una habitación, un edificio, o un conjunto de edificios).

Red WAN: WAN es la sigla de Wide Area Network (“Red de Área Amplia”). El concepto se utiliza para nombrar a la red de computadoras que se extiende en una gran franja de territorio, ya

sea a través de una ciudad, un país o, incluso, a nivel mundial. Un ejemplo de red WAN es la propia Internet.

Software: Se conoce como software1 al equipo lógico o soporte lógico de un sistema informático, que comprende el conjunto de los componentes lógicos' necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos que son llamados hardware.

Los componentes lógicos incluyen, entre muchos otros, las aplicaciones informáticas, tales como el procesador de texto, que permite al usuario realizar todas las tareas concernientes a la edición de textos; el llamado software de sistema, tal como el sistema operativo, que básicamente permite al resto de los programas funcionar adecuadamente, facilitando también la interacción entre los componentes físicos y el resto de las aplicaciones, y proporcionando una interfaz con el usuario.

Software Malicioso: El software malicioso, también conocido como programa malicioso o malware, contiene virus, spyware y otros programas indeseados que se instalan en su computadora, teléfono o aparato móvil sin su consentimiento.

Software P2P: Las aplicaciones P2P (peer to peer) son programas que permiten el intercambio de archivos entre internautas. Los más conocidos son sin dudas LimeWire, Kazaa, Edonkey y Emule

Trazabilidad: El término trazabilidad es definido por la Organización Internacional para la Estandarización A la hora de tener que entender la trazabilidad de un producto que se mueve a través de su cadena de suministro o de su rama logística, el concepto de trazabilidad se divide en dos tipos:

Trazabilidad Interna, es obtener la traza que va dejando un producto por todos los procesos internos de una compañía, con sus manipulaciones, su composición, la maquinaria utilizada, su turno, su temperatura, su lote, etc., es decir, todos los indicios que hacen o pueden hacer variar el producto para el consumidor final.

Trazabilidad Externa, es externalizar los datos de la traza interna y añadirle algunos indicios más si fuera necesario, como una rotura del embalaje, un cambio en la cadena de temperatura, etc.

Usuario: Según la Real Academia Española, un usuario es aquel que usa algo o que usa ordinariamente algo. Sin embargo, esto se opone a los conceptos de la Web semántica, Web 2.0 y 3.0, ya que la realidad actual prima a los ciudadanos como emisores y no solo como receptores que «usan» los medios. Es preferible, por tanto hablar de actores, sujetos, ciudadanos, etc. para referirse a las personas que interactúan en las redes digitales.

BIBLIOGRAFÍA

(ISO), O. I. (2005). *Gestión y administración | Subcategoría: Calidad.* Obtenido de http://www.revistavirtualpro.com.sibulgem.unilibre.edu.co:2048/biblioteca/glosario---iso27000-es#sthash.sKphQiWB.dpuf: http://www.revistavirtualpro.com.sibulgem.unilibre.edu.co:2048/biblioteca/glosario---iso27000-es

Gestión de Riesgo en la Seguridad Informática. (2014). Obtenido de https://creativecommons.org/licenses/by-nc-sa/3.0/es/

M., Jeimy J. Cano. (2014). *Inseguridad de la información.* Recuperado el 30 de octubre de 2016, de Repositorio Virtual unilibre: http://ebooks.alfaomegagrupoeditor.com.sibulgem.unilibre.edu.co:2048/product/inseguridad-de-la-informacin

Ministerio de Telecomunicaciones . (s.f.). Obtenido de http://www.mintic.gov.co/gestionti/615/w3-article-5482.html

Ministerio TIC . (2014). *Modelo de seguridad y privacidad de la informacion* . Bogota , colombia.

Telecomunicaciones, M. d. (14 de julio de 2011). *Documento normas conpes* . Obtenido de http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf: http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf https://protejete.wordpress.com/gdr_principal/retos_seguridad

Ernst & Young realiza encuesta sobre "seguridad de la información"; [Source: Business Wire Latin America]

http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003Mas Importante

Infografía

Cisco, Presentación de información diversas fuentes, 2008. http://www.dinero.com/negocios/telecomunicaciones/colombia-tiene-mejorar-seguridad-informatica_50693.aspx. [Links]

www.eltiempo.com/tecnologia/enter/actualidad_a/home/colombia-debil-en-seguridad-informatica_4393234. http://polux.unipiloto.edu.co:8080/00002024.pdf

ANEXOS

- ENCUESTA
- PLAN DE MEJORA MC_PR_001_MEJORA_CONTINUA_APPS-A59H7Zv8 (1).pdf
- Guía de Gobierno en Línea - GEL, lineamientos por MINTIC, Marco de Seguridad y Privacidad de la Información. Ver documento "00_articles-5482_Modelo_Seguridad.pdf"