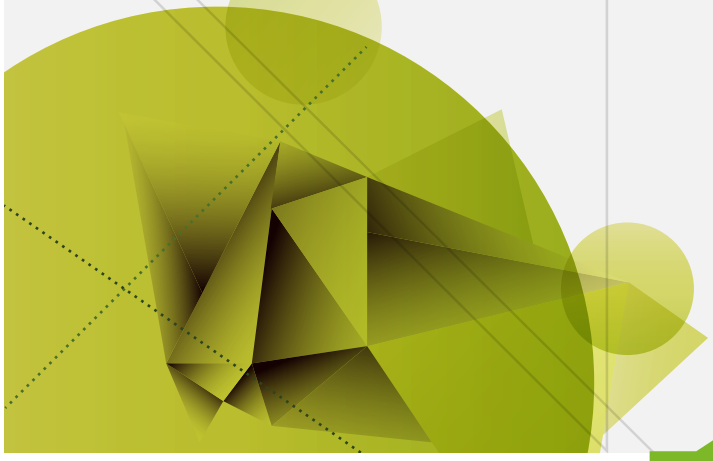
Sistema de Gestión de la Seguridad Informática



Autor: Ricardo Alfredo Lopéz

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

Sistema de Gestión de la Seguridad Informática / Ricardo Alfredo Lopéz, / Bogotá D.C., Fundación Universitaria del Área Andina. 2017

978-958-5455-74-0

Catalogación en la fuente Fundación Universitaria del Área Andina (Bogotá).

Edición:
Fondo editorial Areandino
Fundación Universitaria del Área Andina
Calle 71 11-14, Bogotá D.C., Colombia
Tel.: (57-1) 7 42 19 64 ext. 1228
E-mail: publicaciones@areandina.edu.co
http://www.areandina.edu.co

Primera edición: noviembre de 2017

Corrección de estilo, diagramación y edición: Dirección Nacional de Operaciones virtuales
Diseño y compilación electrónica: Dirección Nacional de Investigación

Hecho en Colombia
Made in Colombia

Sistema de Gestión de la Seguridad Informática

Autor: Ricardo Alfredo Lopéz

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

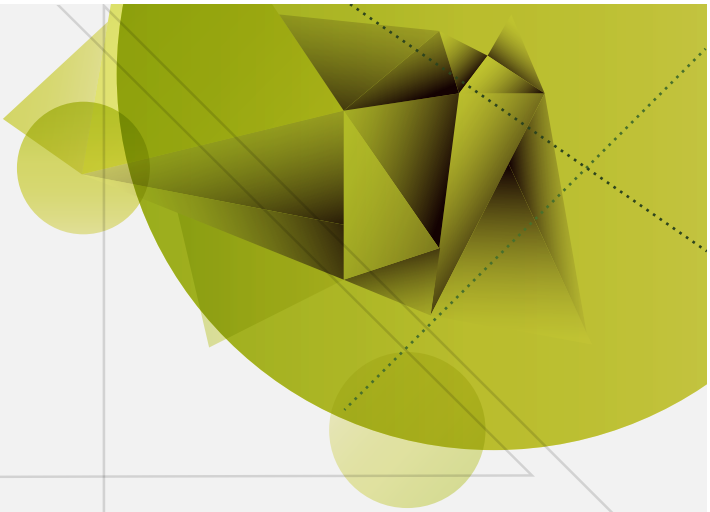
Índice

Índice

1

Unidad 1

Definiciones y conceptos



Sistema de Gestión de la Seguridad Informática

Autor: Ricardo López

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

Introducción

La información es el centro del poder de una empresa, en el mundo moderno se consideran activos de la organización. Su versatilidad da cuenta de los diferentes procesos que constituyen el ser y hacer de la actividad y funcionamiento empresarial. La información se estructura de datos que provienen de diferentes fuentes y que circulan a través de las bases y las redes cibernéticas, transformando las velocidades y espacialidades de su acceso y utilidad, pero que a su vez, la expone a niveles de riesgo y amenaza que deben ser evaluados y controlados de manera técnica y gerencial para controlar de manera eficaz los niveles de vulnerabilidad.

Estos riesgos están asociados con el creciente uso del internet en cada una de las tareas cotidianas de las personas y las organizaciones, tales como las transacciones comerciales, el acceso a servicios, la movilidad financiera y los trámites en general. Acciones que requieren cada vez, unos niveles óptimos de seguridad, pues implican la disponibilidad de datos tanto personales como empresariales de alta privacidad. La seguridad que se ofrezca es determinante en la construcción de confianzas que se reflejan necesariamente en la rentabilidad y el crecimiento de una empresa.

Un incidente de seguridad informática puede generar impactos negativos en una empresa, afectando profundamente su imagen corporativa con sus correspondientes consecuencias en el relacionamiento con el cliente y con la competencia dentro del sector, además de la recurrencia en gastos, generalmente de un alto monto, para subsanar el daño ocasionado.

La gestión en seguridad informática, gira en torno a tres ejes estructurantes, a saber: la disponibilidad, la integridad y la confiabilidad de los datos. La fortaleza de una empresa está ligada a su posibilidad de manejar de manera eficaz y eficiente los datos y de disponer de ellos cuando y donde se requieran, datos que a su vez sean verificables y completos y que además no estén a disposición de personal no autorizado. Estos son los factores que se evalúan en los procesos de gestión de seguridad informática y que se convierten en una de las mejores inversiones de una empresa, inversión que se traduce en su certificación internacional y también en una imagen de confiabilidad para el cliente.

En este sentido, los Estados de todo el mundo han activado sus alarmas frente a este tema y se ha venido consolidando una robusta normatividad y unas reglas de juego para las entidades, tanto públicas como privadas, que regulen el manejo de la información y le garanticen al usuario unas mínimas medidas de seguridad para sus datos e información en general. Poco a poco, todos los países han comenzado a reglamentar la certificación en calidad a nivel local y aunque el proceso también ha sido lento para las empresas, los niveles de concientización y la certeza de los riesgos han permitido un avance significativo en la implementación de la Gestión de Sistemas de Seguridad Informática.

El desarrollo de esta unidad y la lectura analítica del módulo permitirá un acercamiento a las definiciones y conceptos básicos para entender y construir un SGSI. Las relaciones normativas que se han establecido a nivel global y su incidencia en nuestro país.

U1 Metodología

La unidad está divida en 5 temas, cada una de las cuales cuenta con lecturas y documentales que ofrecen el aporte teórico correspondiente al tema, acompañado de ejercicios de aplicación que facilitan el proceso de aprendizaje. Dichos ejercicios requieren que el estudiante, cuente con la documentación de una empresa (real o ficticia) sobre la cual aplicará los conceptos aprendidos.

Al final de la unidad tendrá los insumos iniciales para consolidar un ejercicio de evaluación en la gestión de seguridad de la información de dicha empresa y esta se constituirá junto al test final en su nota de módulo.

U1

Desarrollo temático

Definiciones y conceptos

Información como activo

Según la norma ISO 27000, la información se constituye un activo de las entidades, organizaciones o empresas cualquiera sea su tamaño o función social. Definirse como activo, requiere hacer una medida de valoración que en este caso es proporcional al impacto de su pérdida o manipulación mal intencionada.

La información está constituida de datos, estos permiten identificar elementos o personas y componen una serie de sistemas que permiten el funcionamiento de la organización.

Es importante tener claridad de la información que maneja cada dependencia de una empresa y priorizar su nivel de importancia y confidencialidad.

Escoja tres dependencias de su empresa y realice un listado de la información que maneja (asociada a clientes, productos, personal, mercado, producción, etc.) y organícelas de acuerdo a su prioridad de confidencialidad.

Definición de Sistema de Gestión de Seguridad Informática (SGSI)

El SGSI es un proceso sistemático, protocolizado y manejado por todos los miembros de la empresa que permite la confiabilidad, integridad y disponibilidad de la información de la misma.

El SGSI se ha venido implementando desde los mismos comienzos de la información masiva, sin embargo fue en la década de los 90 que se inició el diseño de estrategias y metodologías para su implementación, siendo Gran Bretaña y los Estados Unidos líderes en el tema.

El primer documento consolidado sobre gestión de seguridad de la información fue publicado por la BSI (British Standards Institution) conocido como la norma BS 7799 donde se compilan un conjunto de buenas prácticas para la SGSI pero fue en la versión de 1998 cuando se establecen los términos y requisitos para certificación. En el año

2000 la ISO (International Organization for Standardization) estandarizó estas dos normas como ISO 17799.

Actualmente todas las empresas europeas y norteamericanas se encuentran certificadas. Sin embargo, en los países latinoamericanos se han presentado obstáculos de orden cultural, económico y normativo para su implementación.

Pilares de la seguridad de la información

La seguridad de la información según la ISO/IEC 27001 se basa en tres pilares fundamentales la confidencialidad, la disponibilidad y la integridad, estos factores se deben garantizar en una adecuada gestión de seguridad de la información.

Confidencialidad de la información

El uso cada vez mayor de la red requiere la circulación de información y datos tanto de empresas como de ciudadanos del común. Cualquier tipo de consulta, transacción y acceso a la web deja una huella de nuestra identificación que queda perennemente en el sistema.

Desde la huella digital, hasta la IP así como datos personales pueden ser de libre acceso a cualquier persona sino se contará con un SGSI que protegiera dicha información disminuyendo su vulnerabilidad.

El derecho a la confidencialidad se ha normatizado a través de diferentes leyes, en el caso de Colombia se cuenta con la Ley Estatutaria de protección de datos personales 1581 de 2012 en la cual se desarrolla el derecho constitucional que tienen todas las personas de conocer, actualizar y rectificar los datos que se hallan recogido sobre ellas.

Las organizaciones deben garantizar la confidencialidad de los datos de sus clientes, su personal y de sus productos, para ello es fundamental el uso de técnicas de control de acceso a los sistemas y el cifrado de la información confidencial.

Esto involucra un monitoreo del manejo de claves, del control del personal que tienen acceso quienes deben firmar compromisos de confidencialidad con su contratante.

La confidencialidad es uno de los factores de mayor riesgo y más complejos de asegurar ya que la información es manejada por el eslabón más débil de la cadena, el usuario, quien por error, omisión o con conocimiento de causa puede dejar expuesta la información vulnerando la organización.

Disponibilidad de la información

La disponibilidad de la información hace referencia al almacenamiento de la información y su accesibilidad al usuario, es la posibilidad de tener la información en el tiempo y espacio requerido. Brindar la información, mantener actualizado el sistema y facilitar su acceso asegura enormes beneficios para la empresa. Sin embargo, debe optimizarse el control de riesgos y disminuir la vulnerabilidad de este flujo. Es en este punto, que la seguridad a través de contraseñas y permisos toma relevancia.

Pero no nos podemos quedar ahí se debe analizar desde los factores de riesgo físico que puedan llegar a impedir el acceso a la información como son robos, fallos eléctricos, riesgos por desastres naturales, ataques de denegación de servicios, ataques terroristas, asonadas, y demás factores que impidan el acceso a la información, como también factores de riesgo Lógico como son

malware, secuestradores de información ransomware, escalamiento de privilegios y destrucción de la data.

Integridad de la información

La integridad hace referencia a la inmutabilidad de la información por personal no autorizado, da cuenta de la certeza de los datos que sean precisos, válidos y coherentes.

Un incidente en la integridad de la información puede resultar nefasto para la empresa, un cambio en el flujo de procesos o de formulación tendría un costo demasiado alto.

Por tanto, el control de la integridad de datos y su eficaz protección son fundamentales en el SGSI.

La integridad es el factor más importante de la seguridad de la información ya que de nada sirve una información disponible y confidencial si su integridad ha sido vulnerada es decir no es exacta ni valida.

Para garantizar la integridad se han desarrollado una serie de algoritmos y certificados digitales, firmas digitales que en un alto porcentaje garantiza la integridad de la data.

Marco normativo nacional e internacional

Entidades Normalizadoras	
IUT-T	International Telecommunication Union, las comisiones de estudio del sector de normalización de las telecomunicaciones, quienes elaboran recomendaciones UIT para las TIC con el objeto de estandarizar un lenguaje común para su uso global.
ISO / IEC	International Organization for Standarization. Organización encargada de crear normas de estandarización internacional. La ISO/IEC es un marco internacional de las prácticas de seguridad informática reconociendo la información como un activo de gran valor para las empresas.
CEN/CENELAC	Comité europeo de normalización electrónica que junto a la ETSI produce normas aplicables a nivel mundial en torno a las TIC
ICONTEC	Instituto Colombiano de normas técnicas y certificación. Es el organismo que emite las certificaciones de calidad en nuestro país.
BSI	British Standards Institution (BSI), institución Británica encargada de la creación de normas para la estandarización de procesos, centra sus actividades en la certificación, auditoria y formación de normas. Es una entidad colaboradora de la ISO y proveedora de normas.

Tabla 1
Fuente: propia

Normas de Evaluación y Certificación
TCSEC: Trusted Computer Security Evaluation Criteria. En la década de los 80´el departamento de defensa de Estados Unidos publicó El Libro Naranja (Orange Book) en el que se describen criterios de evaluación en seguridad informática agrupadas en 7 clases donde se evalúan cuatro aspectos: Política de seguridad, imputabilidad, aseguramiento y documentación.
ISO / IEC: Dentro de su marco normativo, se certifica: Medidas administrativas, medidas físicas, marco legal de la evaluación y calidad intrínseca de algoritmos de cifrado, así como los perfiles de protección (tarjetas inteligentes, sistemas operativos, acceso basado en roles y cortafuegos).
ITSEC/ITSEM: Estándar Europeo de evaluación y certificación. Los criterios de evaluación se reúnen en el ITSEC y las metodologías de implantación en el ITSEM. Este estándar evalúa: La funcionalidad (conjunto de funciones de seguridad), la confianza (Efectividad y corrección). Las partes implicadas en la certificación son: Patrocinador, productor, instalaciones de evaluación, Comisión Nacional de certificación (Reino Unido, Francia y Alemania).
BSI entidad Europea encargada del desarrollo de normas para la gestión de la seguridad de la información, gestión de la calidad, gestión medio ambiental entre otros.

Tabla 2
Fuente: propia

Familia de normas ISO/IEC 27000

La norma ISO/IEC es una serie de normas en torno al SGSI donde se definen términos, procesos de implementación y evaluación. Los rangos de numeración van de 27000 a 27019 y de 27030 a 27044.

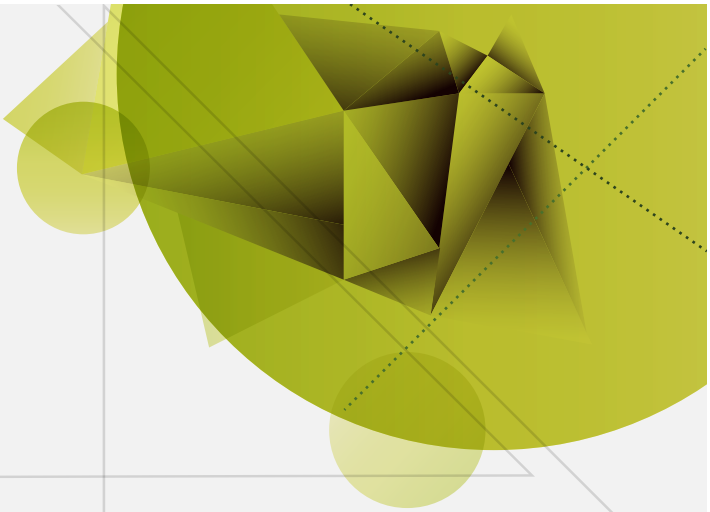
Norma ISO/IEC	Fecha	Contenido
27000	2008	Términos y definiciones que estandarizan el vocabulario de la serie.
27001	2005, 2013 ultima actualización	Sistema de Gestión de Seguridad de la Información. SGSI. Norma certificable.
27002	2005, 2007, 2013 última	Guía de buenas prácticas. Enumera los objetivos de control y controles a desarrollar en cuanto a seguridad informática. Antigua ISO 17799 derivada de BS799
27003	2010	Guía de implementación de SGSI
27004	2009	Especifica métricas y técnicas de medidas aplicables para determinar la eficacia del SGSI
27005	2008, Revisada 2011	Diseñada para ayudar a la aplicación de la seguridad informática desde un enfoque de gestión de riesgos.
27006	2007	Requisitos para la acreditación de entidades de auditoria y certificación.
27007	2011	Guía de auditoria.
27011	2008	Implementación del SGSI en el sector de telecomunicaciones.
27017	2015	Guía de seguridad para Cloud Computing, (computación en la nube).
27031	2010	Guía de continuidad de negocio en cuanto a tecnologías de información y comunicaciones.
27034	2012	Guía de seguridad en aplicaciones.
27035	2011	Guía de gestión de incidentes de seguridad
27799	2008	Estándar de gestión de seguridad de la información en el sector sanitario aplicando ISO 17799 (Salud informática).

Tabla 3
Fuente: propia

1

Unidad 1

Sistema de Gestión de Seguridad de la Información



Sistema de Gestión de la Seguridad Informática

Autor: Ricardo López

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

Introducción

Reconocer la importancia de la implementación del SGSI es uno de los retos para los países latinoamericanos, dimensionar el valor de la información como activo sustancial de la empresa y generar la responsabilidad social de la protección de la misma para beneficio de la organización, sus clientes y proveedores debe ser el primer paso para la implementación de metodologías y herramientas que busquen la óptima disponibilidad, integridad y confiabilidad de la información.

En este módulo se brindaran las bases metodológicas para la implementación del SGSI en las empresas, la estructura del proceso y las herramientas disponibles para su implantación.

U1 Metodología

Está cartilla aborda la unidad 2 del módulo y se compone de tres temas estructurales, los cuales cuentan con lecturas y documentales que ofrecen el aporte teórico correspondiente a cada tema, acompañado de ejercicios de aplicación que facilitan el proceso de aprendizaje. Dichos ejercicios requieren que el estudiante, cuente con la documentación de una empresa (real o ficticia) sobre la cual aplicará los conceptos aprendidos y que se describe en la guía de actividades.

Al final de la unidad tendrá los insumos iniciales para consolidar un ejercicio de evaluación en la gestión de seguridad de la información de dicha empresa y ésta se constituirá junto al test final en su nota de módulo.

En esta semana se realizará un quiz que evaluará las dos primeras semanas de desarrollo del módulo.

U1

Desarrollo temático

Sistema de Gestión de Seguridad de la Información

Metodologías de implantación

El proceso de implantación del SGSI, se compila en la norma 27001 – 27002 donde se plasman las etapas que deben abordarse en el momento de elaborar un plan estratégico de SGSI. Cabe resaltar que la norma establece la necesidad y urgencia de elevarlo a categoría de política de seguridad con el fin de involucrar a todos los estamentos de la organización pero especialmente a los de alto nivel quienes tienen la potestad de tomar las decisiones pertinentes.

La norma presenta un enfoque basado en procesos, bajo el modelo de procesos PHVA, "Planificar- Hacer- Verificar - Actuar" que se aplica para a todos los procesos del SGSI.

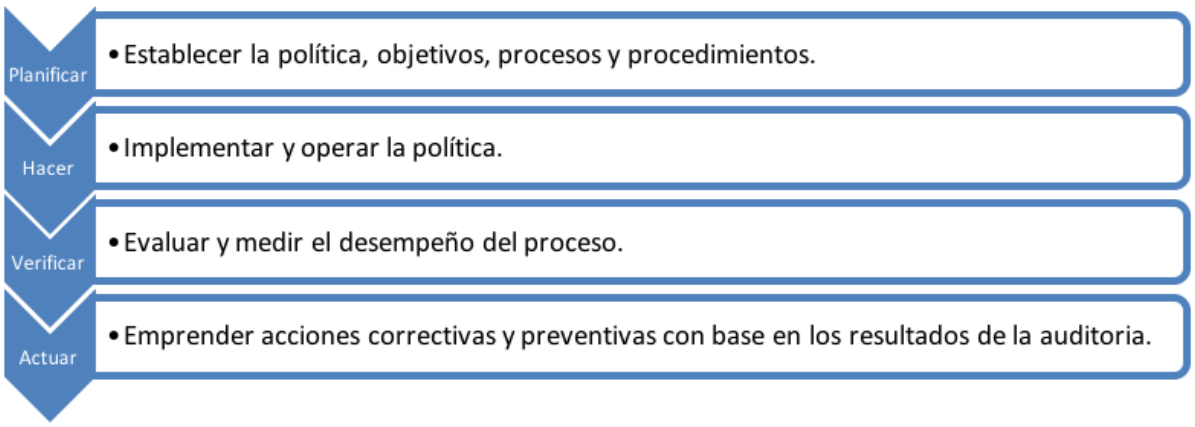


Figura 1
Fuente: propia

Las etapas del enfoque basado en procesos son:

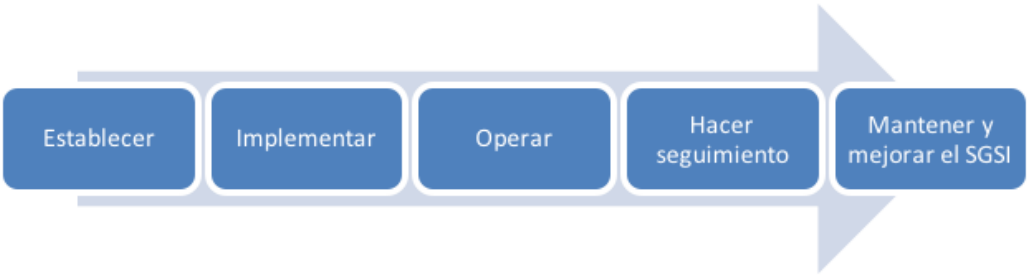


Figura 2
Fuente: propia

Establecimiento del SGSI:

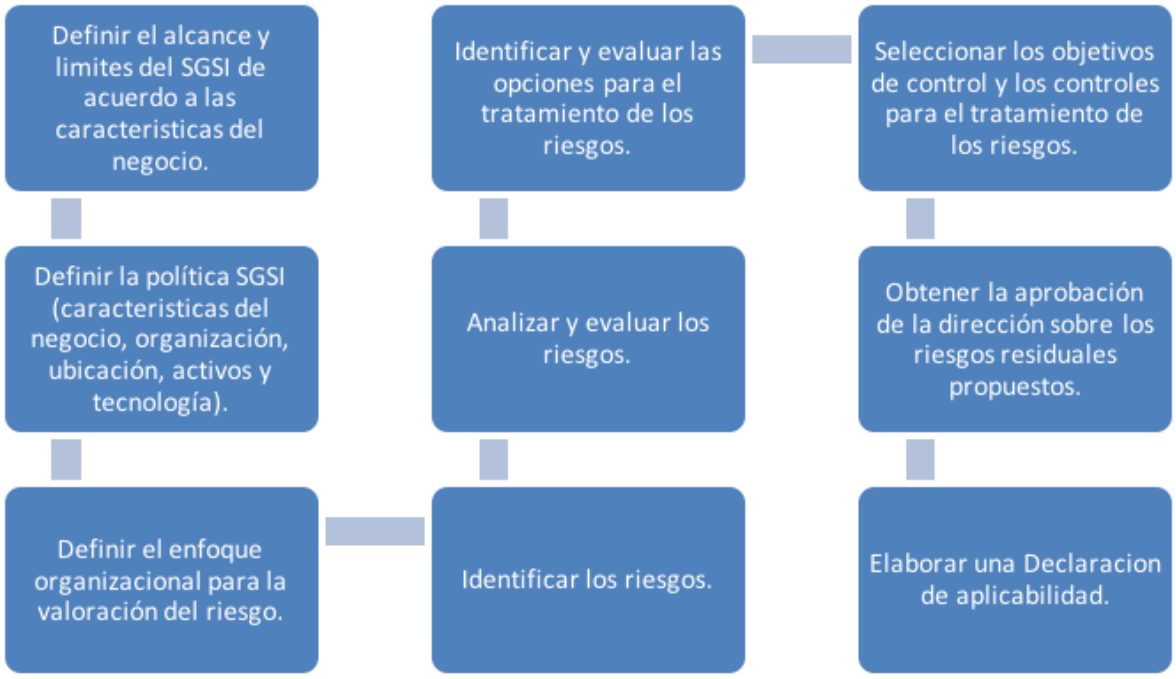


Figura 3
Fuente: propia

Implementación y operación del SGSI:

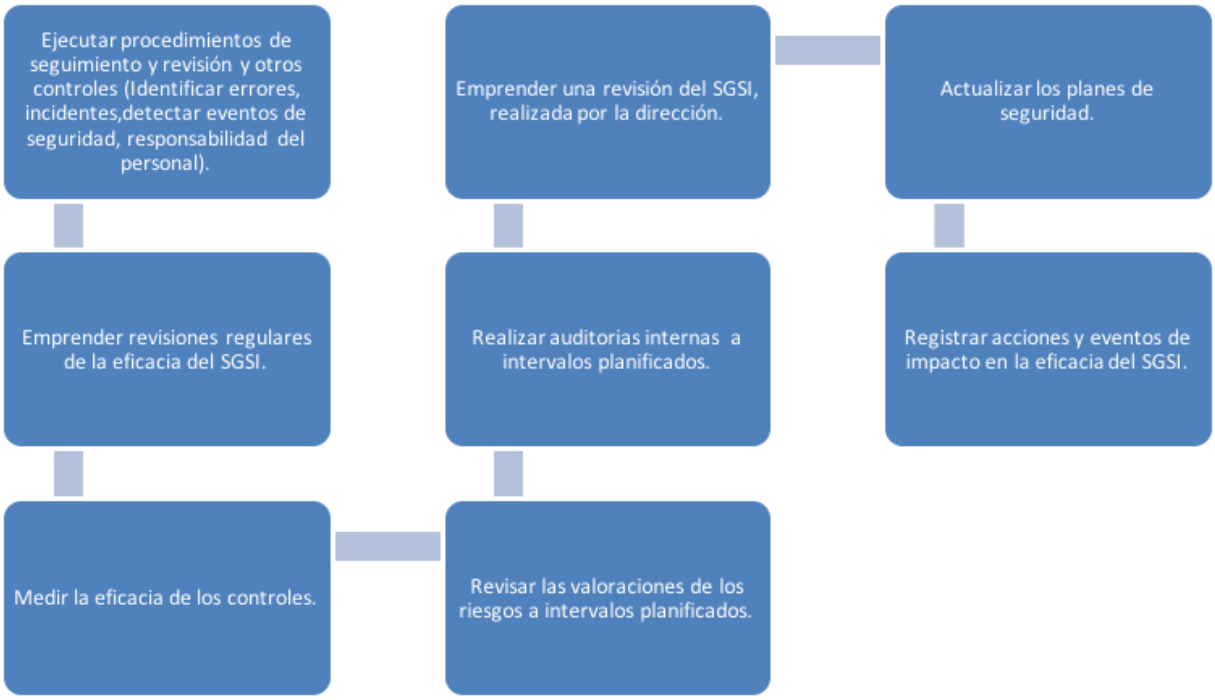


Figura 4
Fuente: propia

Seguimiento y revisión del SGSI:

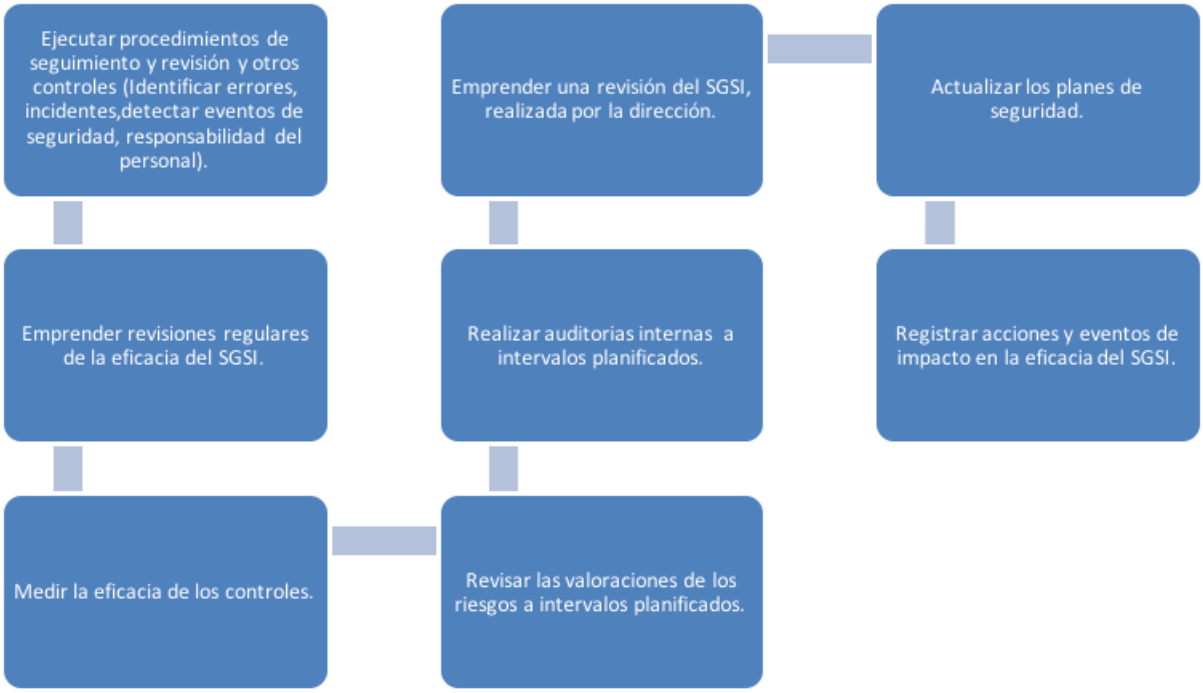


Figura 5
Fuente: propia

Mantenimiento y mejora del SGSI:

Figura 6
Fuente: propia

Desafíos sistema de gestión de seguridad de la información

Entre sus desafíos están la regulación de todas las empresas y organizaciones tanto estatales como privadas, certificando en seguridad de la información a todos los usuarios y poseedores de estos activos.

Esto con miras a proporcionar ventajas competitivas, independencia en el manejo del recurso y la implementación de las normas y leyes. Para ello es importante cualificar personal que brinde el apoyo técnico y la auditoria pertinente, además de consolidar la norma para incorporar a todas las organizaciones y por último convertirla en una política gerencial de cada organización.

La implementación de SGSI no es un gasto o perdida es en realidad una inversión.

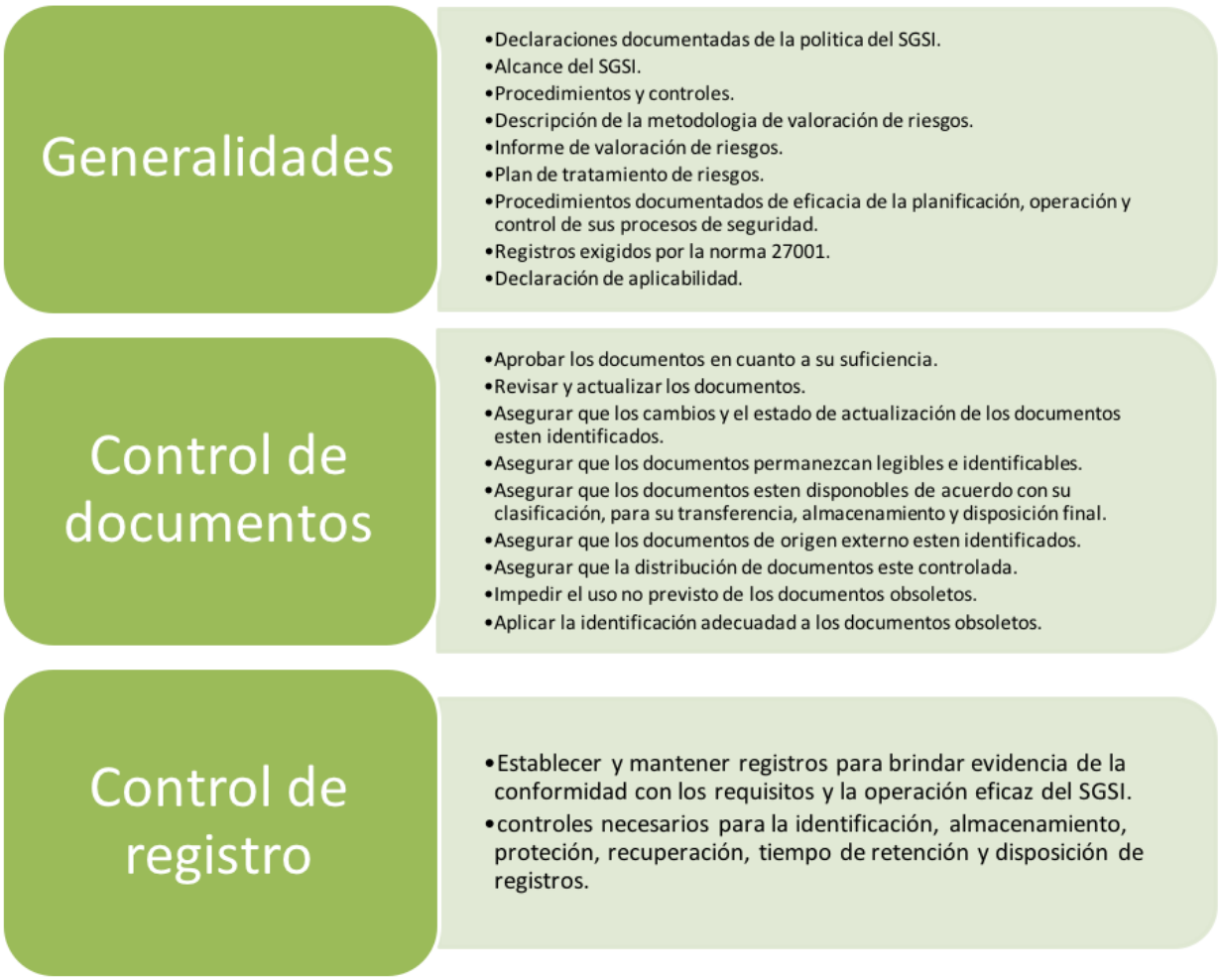


Figura 7. Requisitos de documentación para certificación del SGSI
Fuente: propia

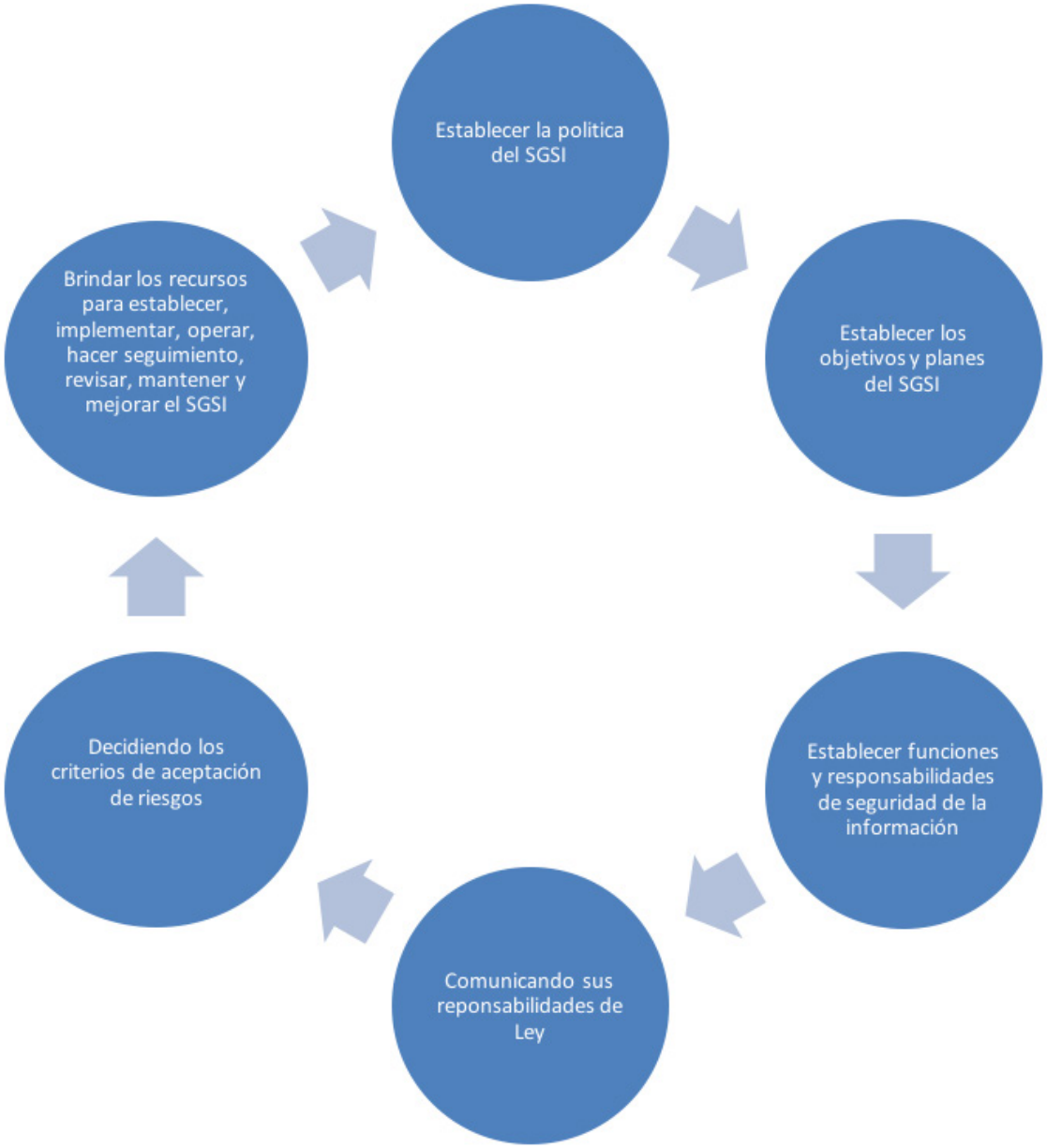


Figura 8. Responsabilidad de la dirección
Fuente: propia

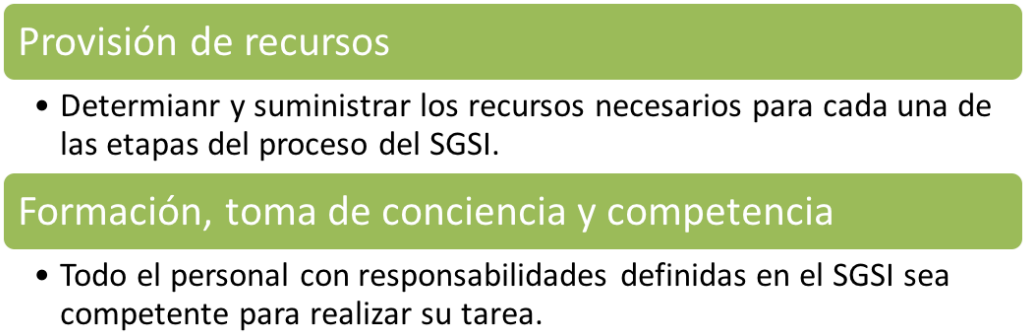


Figura 9. Gestión de recursos
Fuente: propia

Auditorías internas del SGSI

La auditoría debe ser planificada y con intervalos regulares de acuerdo a la priorización de la información de cada área de la organización. La selección de auditores debe asegurar imparcialidad y objetividad.

Revisión de SGSI por la dirección

La revisión debe ser regular y planificada con el objeto de evaluar la conveniencia, suficiencia y eficacia del SGSI. Se realiza con base en los informes de auditoría y la retroalimentación de las partes involucradas y debe dar como resultado un documento de informe con las mejoras, actualizaciones modificaciones y recursos necesarios.

Mejoras del SGSI

La mejora continua del SGSI debe generar acciones correctivas y preventivas revisadas por la dirección y las áreas involucradas.

Herramientas utilizadas en la gestión de seguridad de sistema de información

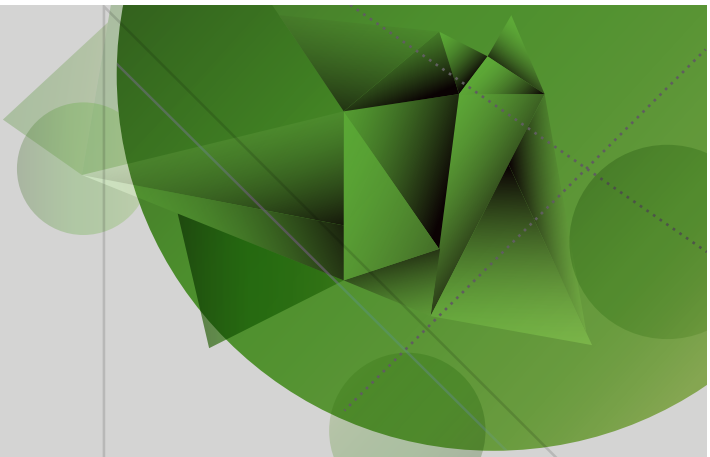
Existen múltiples herramientas utilizadas en la implantación del SGSI, a continuación se hará un listado de las más relevantes en el mercado:

Herramienta	Descripción
GESCONSULTOR	Plataforma que integra los elementos para la implantación del SGSI. GESDATOS Software S.L.
AGGIL	Sistema de información SaaS.
ePULPO	Plataforma de Unificación Lógica de los Procesos Organizativos.
GlobalSuite	Herramienta de la consultora española Audisec.
SECURIA SGSI	Plataforma automática del SGSI.
Inmuno SGSI	Automatización del cumplimiento de requisitos del SGSI.
Bro	Sistema de detección de intrusos, código abierto NIDS que monitorea el tráfico de red y busca comportamiento anómalo del tráfico.
Nagios	Monitoreo de host y de red que informa interrupciones al usuario.
OSSEC HIDS	Sistema de prevenciones y detección de intrusiones de host de código abierto.
OSSIM	Gestión de la información de seguridad de código abierto. Proporciona un conjunto de herramientas de control.

2

Unidad 2

Protección de datos, privacidad e intimidad



Sistema de Gestión de la Seguridad Informática

Autor: Ricardo López

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

Introducción

¿Qué entendemos por privacidad? ¿Qué información consideramos privada? ¿y quién podría acceder a ella? este, es un tema fundamental dentro del contexto global del internet; las conexiones en línea transformaron las dimensiones espacio temporales de los individuos y organizaciones, transmutando profundamente las relaciones sociales, desde las relaciones íntimas e interpersonales, hasta la relación cliente y proveedor. Claro, dentro de las múltiples relaciones humanas que se desarrollan a través del mundo del internet, el acceso a la información queda plenamente al descubierto, pues el acceso a ella es mucho más sencillo y por ende, más vulnerable, motivo por el cual, no podría menos que pensarse en una regulación normativa que merme los impactos negativos y regule la incidencia y el nivel de privacidad e intimidad de los datos.

Tanto si son personales u organizacionales, la información en la red se ve expuesta a múltiples amenazas que atentan contra su disponibilidad, integridad y confiabilidad, dentro de los procesos de recolección, tratamiento, circulación, acceso y uso de la información.

Las implicaciones de este tipo de incidentes pueden ser nefastas para una empresa o persona. Pues actualmente circula por la red, información absolutamente privada (como puede se lo concerniente al acceso de cuentas bancarias) que en caso de ser manipulada por personas no autorizadas, podría generar daños irreversibles.

Así bien, tanto a nivel internacional como nacional, se han consolidado una serie de normas que circunscriben este tipo de incidentes como delitos punibles y promueven la protección de la información, reiterando a las empresas y organizaciones la obligación que tienen, frente al manejo de los datos y la información. La implantación de un sistema de gestión de la seguridad de la información (SGSI) se convierte en un requisito indispensable de competitividad para todo tipo de empresa.

En este entendido, la siguiente cartilla le ayudará a vislumbrar un escenario jurídico que le permita comprender la importancia de la protección de datos en el estado colombiano, así como también la trascendencia que implica una regulación normativa frente a los temas de la propiedad Intelectual y la propiedad patrimonial.

U2 Metodología

La unidad está divida en cuatro temas, cada uno de las cuales cuenta con lecturas y documentales que ofrecen el aporte teórico correspondiente al mismo, acompañado de ejercicios de aplicación que facilitan el proceso de aprendizaje y algunos apartes de casuística.

Al final de la unidad el estudiante contara con los insumos esenciales para poder proteger y respetar lo expresado por la normatividad colombiana con respecto a la protección de datos, la privacidad y la intimidad, así como también conocerá el manejo básico que debe efectuarse frente al tema de la propiedad intelectual.

U2

Desarrollo temático

Protección de datos, privacidad e intimidad

La protección de datos en el Estado colombiano: Escenario General

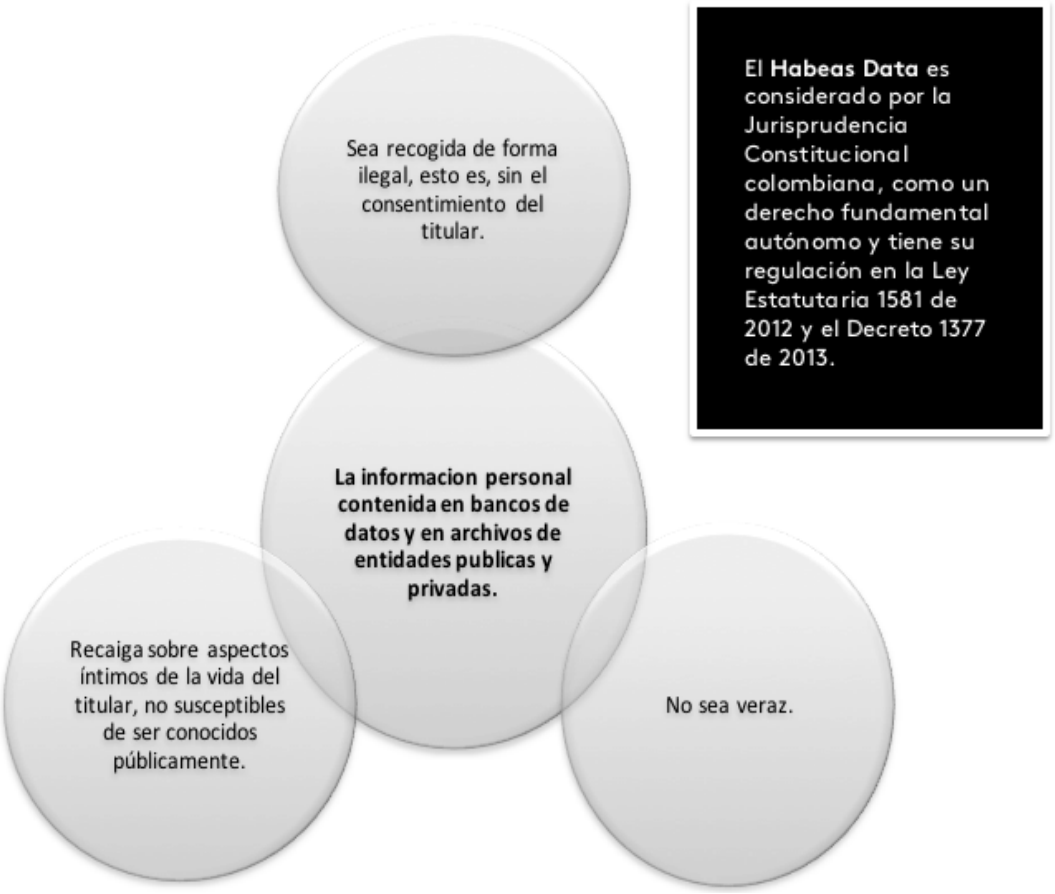
El artículo 15 de la Constitución Política de Colombia, señala que todas las personas tienen derecho a su intimidad personal, familiar y a su buen nombre, así como también lo tienen de conocer, actualizar y rectificar lo que de ellas se haya recogido en bancos de datos y en archivos de entidades públicas y privadas, exigiendo de estas últimas el adecuado tratamiento de la información personal dentro del marco del respeto de los derechos constitucionalmente reconocidos.

Lo anterior, como bien sabrán algunos, corresponde al derecho fundamental denominado Habeas Data el cual, desde un inicio fue interpretado por la jurisprudencia de la Corte Constitucional de diversas maneras:

1. Como una garantía del derecho a la intimidad.
2. Como una manifestación del libre desarrollo de la personalidad.
3. Como un derecho autónomo.

Aunque suela pensarse que las tres apuntan a lo mismo, debe señalarse que es la última interpretación la que actualmente continua vigente, y es qué considerar el Habeas Data como un derecho fundamental autónomo, implica la no dependencia con los demás derechos fundamentales, incluso cuando su protección involucre la salvaguardia de los otros derechos. En este sentido y como derecho autónomo, el Habeas Data requiere para sí, mecanismos de protección judicial, administrativa e institucional que lo garanticen, asegurando el resguardo integral de los datos personales que se encuentren en bancos de datos y en archivos de entidades públicas y privadas.

Al tenor de la Sentencia T-167 de 2015 de la Corte Constitucional colombiana, el derecho fundamental del Habeas Data puede llegar a verse amenazado o vulnerado, cuando quiera que:



En este sentido y consientes de la vulneración ininterrumpida del derecho del Habeas Data por parte de las entidades públicas y privadas, el Congreso de la Republica decide expedir para el año 2012 la Ley Estatutaria 1581, la cual es reglamentada posteriormente y de manera parcial por el Decreto 1377 de 2013. Recordemos que en una época, era muy común que nos llegara información y publicidad de muchas entidades desconocidas que señalaban nuestro nombre y hasta nuestra dirección de domicilio, así como también lo era que se comunicaran a nuestros números telefónicos, ofreciéndonos servicios y productos sin que nosotros hayamos autorizado previamente dicho manejo de nuestros datos.

La ley Estatutaria 1581 de 2012 y el Decreto 1377 de 2013, tienen aplicación exclusiva sobre la información y datos personales **registrados** en cualquier base de datos que les haga susceptibles de tratamiento por parte de entidades públicas o privadas

En este sentido, cabe señalar que la primera norma (Ley Estatutaria 1581 de 2012) posee un rango jerárquico especial que la ubica por encima de las demás leyes ordinarias, esto, por cuanto trata un derecho fundamental y regula su protección. El objeto de Ley Estatutaria 1581 de 2012 se centra en el desarrolló del derecho constitucional del Habeas Data que reconoce la posibilidad que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política (Ley Est.1582/12).

De esta manera, la ley tiene aplicación sobre la información y datos personales registrados en cualquier base de datos que les haga susceptibles de tratamiento por parte de entidades públicas o privadas en el territorio colombiano, con excepción a lo establecido por las normas y tratados internacionales; así bien, la ley no tendrá aplicación cuando se trate de bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico, cuando las bases de datos y archivos tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo o cuando las bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia, entre otros.

Ahora, el tratamiento que realicen las entidades públicas o privadas sobre la información personal a la que nos hemos referido, requiere la autorización previa e informada del titular. Dicha autorización deberá ser estipulada de tal manera que pueda ser objeto de consulta posterior, siempre que se requiera.

Conforme a lo anterior, la ley prevé únicamente cinco excepciones para el tratamiento de la información, en este sentido la autorización del Titular no será necesaria cuando se trate de información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial, cuando sean datos de naturaleza pública, cuando se trate de casos de urgencia médica o sanitaria, cuando el tratamiento sea autorizado por la ley para fines históricos, estadísticos o científicos y cuando se trate de datos relacionados con el Registro Civil de las Personas.

No acatar la protección integral del **Habeas Data** puede acarrear Sanciones que pueden consistir en multas, suspensión o cierre.

Es importante resaltar que el titular, sus causahabientes o su representante y/o apoderado, podrán presentar reclamos ante el Responsable del Tratamiento o el Encargado del Tratamiento siempre que lo considere necesario para la protección de sus derechos constitucionales. Para esto, la Superintendencia de Industria y Comercio, a través de la delegatura para la Protección de Datos Personales, vigilará a las entidades para

garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la ley y en los decretos reglamentarios.

Para lo anterior, la Superintendencia de Industria y Comercio podrá adelantar investigaciones de oficio o a petición de parte, así como también podrá ordenar medidas para hacer efectivo el derecho de Hábeas Data e imponer las sanciones pertinentes, las cuales pueden consistir en:

- Multas de carácter personal e institucional.
- Suspensión de las actividades relacionadas con el Tratamiento.
- Cierre temporal o definitivo de las operaciones relacionadas con el Tratamiento.

De esta manera queda claro que el Habeas Data, como derecho fundamental autónomo cuenta con protección legal propia que permite su amparo integral. Además, debe reiterarse que la Superintendencia de Industria y Comercio está encargada de vigilar el tratamiento de la información que consta en bases de datos y archivos de entidades públicas y privadas; No obstante, cabe resaltar que, para evitar amenazas o vulneraciones a los derechos fundamentales, es indispensable que su titular los conozca, atienda los avisos de privacidad y decida solicitar las medidas correctivas, pues es este principalmente, quien debe velar por sus derechos.

Figura 1
Fuente: www.sic.gov.co/sobre-la-proteccion-de-datos-personales

Propiedad intelectual y propiedad patrimonial

Cuando el artículo 58 de la Constitución Política de Colombia se refiere a la propiedad privada, las personas suelen suponer que este alude únicamente a los bienes tangibles que poseemos (la casa, el carro, el celular, el computador, etc.), no obstante, ignoran la idea de que pueda ejercerse un dominio sobre las creaciones humanas. Para dedicarnos a hablar sobre el tema en comento, es importante hacer una diferenciación sustancial entre los dos campos que comprende la propiedad intelectual.

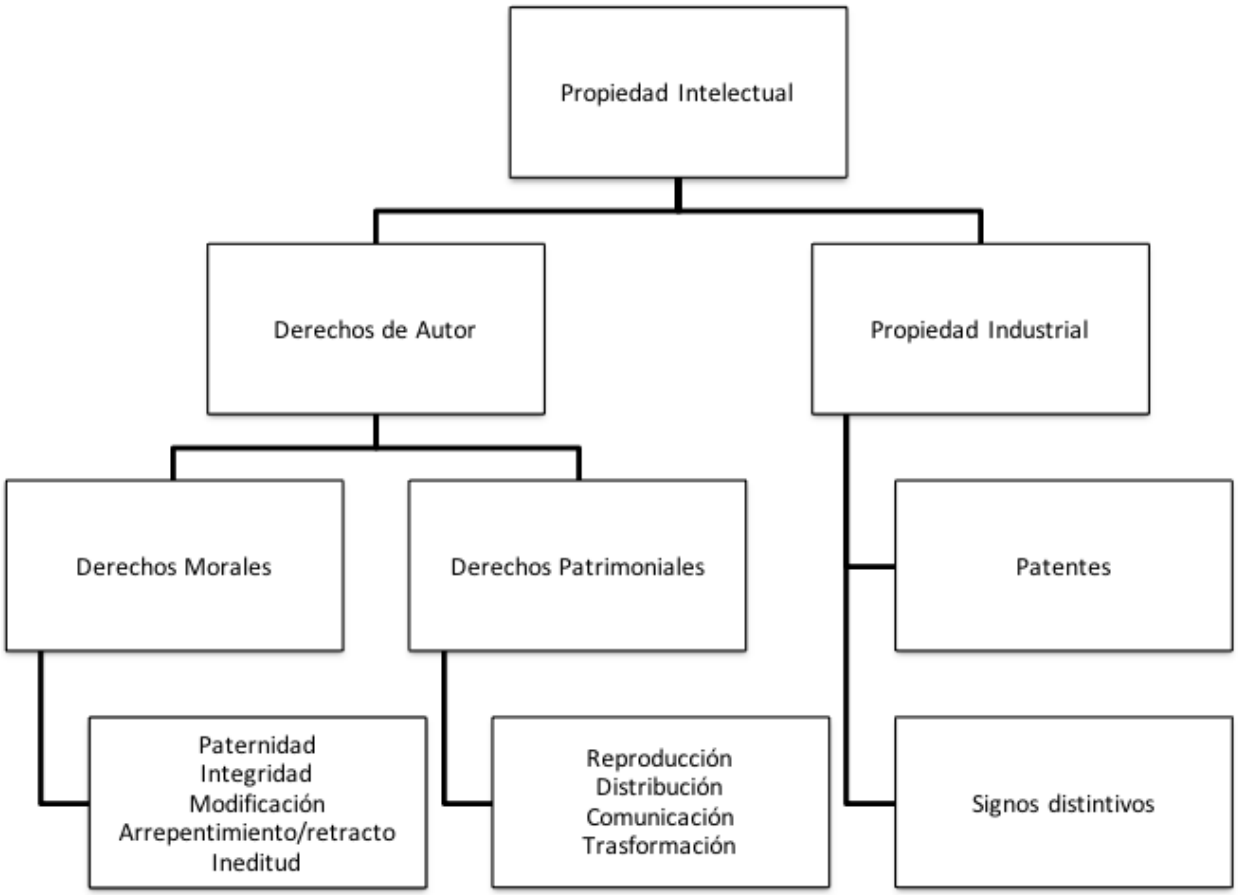


Figura 2
Fuente: propia

El derecho que le asiste los inventores sobre sus obras, ha sido un tema que desde el siglo XIX ha inquietado a los juristas, pues incluso cuando la obra tenga un uso social, es el creador quien en principio debe llevarse el crédito y beneficio de la misma. Así para el año 1883 y el año 1886 (Convenio de París y Convenio de Berna respectivamente) se empieza a pensar en un marco legal que permita la protección integral de los derechos del creador frente a su obra, dando pie a la posterior creación de la Organización Mundial de la Propiedad Intelectual (OMPI), foro de índole mundial al que le corresponde tratar los temas concernientes a la propiedad intelectual (P.I.).

Sobre lo indicado por la OMPI, Colombia ha creado el margen normativo de protección de los derechos de autor y propiedad industrial, instituyendo además entidades de vigilancia, control y protección, como lo es la Dirección Nacional de Derechos de Autor y la Superintendencia de Industria y Comercio. Ahora, resulta indispensable hacer la diferenciación entre lo que son los derechos de autor y la propiedad industrial. Lo primero que debe decirse es que los derechos de autor parten de "toda creación intelectual original de naturaleza artística, científica o literaria, susceptible de ser divulgada o reproducida en cualquier forma" (Decisión andina 351 de 1993 régimen común sobre derecho de autor y derechos conexos) en este entendido, una canción, una foto o un dibujo pueden llegar a ser protegidos por el derecho de autor siempre que cumpla los requisitos que posteriormente trataremos; mientras que la propiedad industrial abarca las patentes (de invención y modelos de utilidad) y los signos distintivos (Nombres comerciales, lemas comerciales, indicación geográfica, marcas, rótulos y enseñas).

El software entendido como un soporte lógico y un conjunto de caracteres, por ejemplo, es una obra que puede llegar a ser protegida por el derecho de autor, siempre que cumpla, al igual que el resto de las obras, con unos principios básicos que se estipulan para la eventual protección por parte de la Dirección Nacional de Derechos de Autor, dentro de los cuales se encuentra:

Figura 3
Fuente: propia.

Protegida una obra, debe entenderse entonces que surgen por antonomasia dos derechos diferentes, los derechos morales (Paternidad, Integridad, Modificación, Arrepentimiento /retracto e Ineditud) y los derechos patrimoniales (Reproducción, Distribución, Comunicación, Trasformación), siendo estos últimos los únicos susceptibles de traspaso (bien sea por venta, donación, etc.).

Así pues, el autor es el único que tiene el derecho de indicar que esa obra es suya (derecho de paternidad) y los terceros deben respetar dicho derecho señalando la autoría ajena, del mismo modo, es el autor el único quien puede modificar su creación, retractarse de ella o mantenerla inédita, porque estos derechos son personalísimos, indelegables, inembargables, intransferibles y perennes. Contrario se encuentra entonces los derechos patrimoniales, como la reproducción de la obra (es decir, fotocopiarla, imprimirla, digitalizarla en masa, etc.) la distribución, la comunicación y transformación, pues el autor puede ceder estos derechos que cuentan con las características de trasferibles, embargables y perecederos (pues se protegen únicamente por la vida del autor más cincuenta años después de su muerte).

Frente a lo último, es importante resaltar que incluso cuando el derecho de paternidad es exclusivo del autor (Para derechos de autor tanto como para propiedad industrial), los derechos patrimoniales se presumen de un tercero, cuando por ejemplo, existe cesión (trasferencia) de derechos, cuando se trata de una obra por encargo, cuando se realiza con base en un contrato de trabajo o cuando existe una relación con una entidad pública.

Sabías que el fotógrafo británico David Slater alego los derechos de autor por una selfie que se tomó un mono indonesio Naruto mientras el fotógrafo se encontraba distraído.

Esta solicitud fue negada por el juez al no existir el principio de "creación intelectual".

Figura 4
Fuente: http://www.reasonwhy.es/actualidad/sociedad-y-consumo/selfies-y-derechos-de-autor-quien-le-pertenecen-las-imagenes_2014-08

Así bien, por ejemplo, cuando se le paga a un pintor por hacer un retrato de la familia, debe tenerse en cuenta que, aunque el autor tenga el derecho de paternidad sobre la obra (es decir, se debe reconocer su autoría), quien puede llegar a vender, distribuir y modificar la obra con fines económicos, será exclusivamente quien contrato el servicio por encargo, pues es este último el dueño de los derechos patrimoniales.

Lo mismo sucede con las obras que se crean a partir de un contrato de trabajo (Ley 23 de 1982), pues aunque la autoría debe ser reconocida al trabajador (creador), los derechos patrimoniales de la obra serán de la empresa. Pensemos entonces en una entidad que ofrece dadivas y beneficios al trabajador que logre crear un sonsonete llamativo para la empresa. Si uno de los trabajadores lo creara y este tuviera un éxito extraordinario, quien se lucraría de los beneficios económicos seria exclusivamente la empresa, pues el trabajador obtendría únicamente el reconocimiento de autoría.

Ahora, frente a la propiedad industrial (decisión 486 de 2000) debe indicarse que se divide en Patentes y Signos Distintivos, entendiendo las patentes como el derecho exclusivo de explotación que le ofrece el Estado (A través de la Superintendencia de Industria y Comercio) al inventor y que como privilegio, puede ser cedido por este. Esta patente debe ser absolutamente novedosa (lo que lo diferencia de un modelo de utilidad el cual parte de una patente para mejorarla), debe poseer un nivel inventivo y una aplicación industrial.

En cuanto a los signos distintivos, como los lemas y nombres comerciales, las indicaciones geográficas, las marcas (Nominativa, evocativa, figurativa, sonora y olfativa, nombre geográfico o certificación) y los rótulos y enseñas, son caracteres que diferencian un servicio o un producto de los demás y su protección implica la protección indiscutible del servicio o producto.

Figura 5
Fuente: propia

Pensemos entonces en el mal que podría generarse si una empresa empezara a producir pastelillos cubiertos de crema negra (de origen dudoso) y fuera empacada en un paquete anaranjado (muy parecido al de chocorramo) y se llamara "Chocoarmo". ¿Podría llegar el consumidor a confundirse y pensar que chocorramo está desmejorando la calidad? Evidentemente, por eso se hace necesaria la protección de los signos distintivos ante la Superintendencia de Industria y comercio, quien posee las facultades investigativas y sancionatorias que ameriten cada caso.

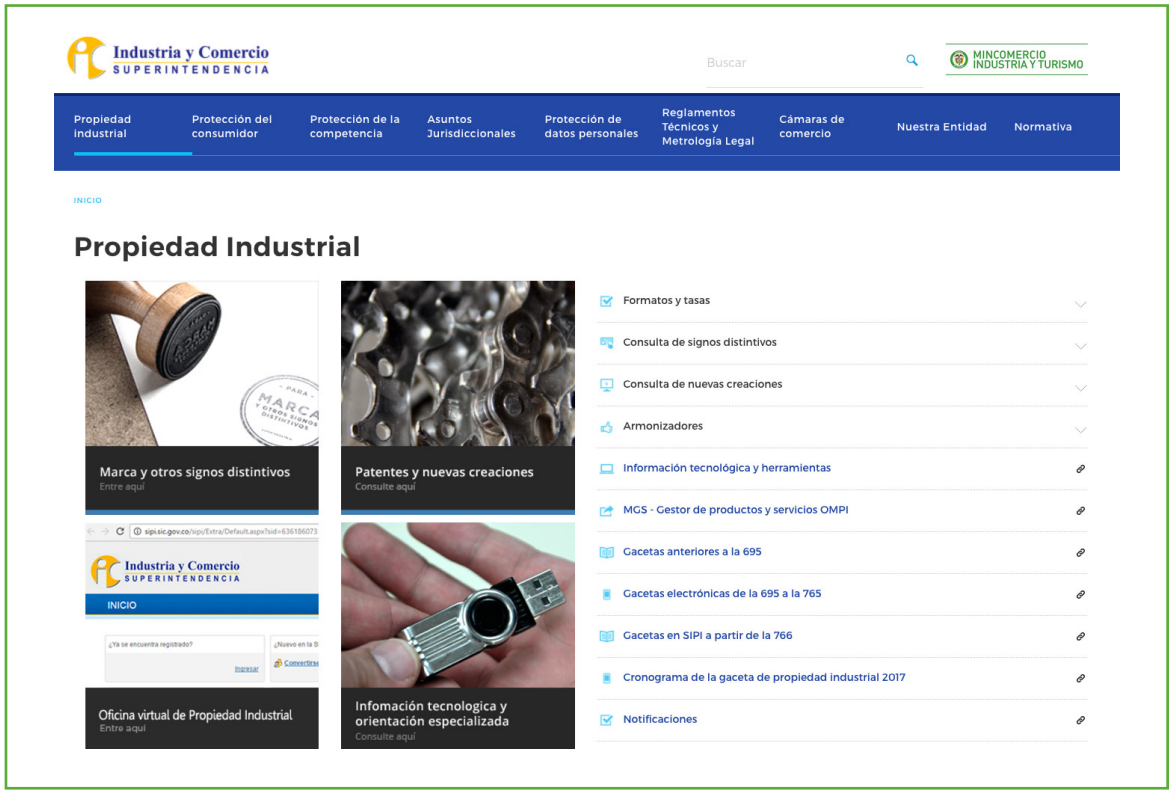


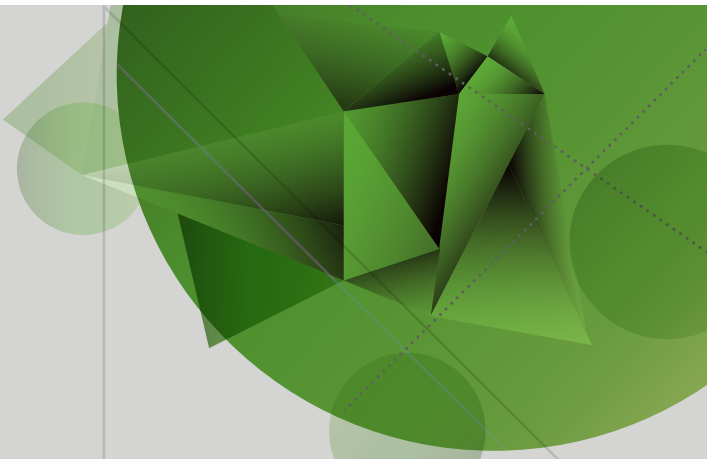
Figura 6
Fuente: www.sic.gov.co/propiedad-industrial

Recuerde que la importancia que denota la protección integral de la propiedad intelectual es indiscutible, pues de esta se derivan derechos económicos, sociales y culturales, así como el derecho de propiedad intelectual como derecho humano, por eso es trascendental que el estudiante sepa cuáles son sus derechos y pueda saberlos proteger. Si es usted una persona interesada en crear, puede visitar la página de la Superintendencia de Industria y comercio (Si se trata de propiedad industrial) o la página de la Dirección Nacional de Derechos de Autor (Si es el caso de Derechos de autor) e inscribir sus creaciones.

2

Unidad 2

La privacidad y el derecho a la intimidad



Sistema de Gestión de la Seguridad Informática

Autor: Ricardo López

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

Introducción

¿Qué entendemos por privacidad? ¿Qué información consideramos privada? ¿y quién podría acceder a ella? este, es un tema fundamental dentro del contexto global del internet; las conexiones en línea transformaron las dimensiones espacio temporales de los individuos y organizaciones, transmutando profundamente las relaciones sociales, desde las relaciones íntimas e interpersonales, hasta la relación cliente y proveedor. Claro, dentro de las múltiples relaciones humanas que se desarrollan a través del mundo del internet, el acceso a la información queda plenamente al descubierto, pues el acceso a ella es mucho más sencillo y por ende, más vulnerable, motivo por el cual, no podría menos que pensarse en una regulación normativa que merme los impactos negativos y regule la incidencia y el nivel de privacidad e intimidad de los datos.

Tanto si son personales u organizacionales, la información en la red se ve expuesta a múltiples amenazas que atentan contra su disponibilidad, integridad y confiabilidad, dentro de los procesos de recolección, tratamiento, circulación, acceso y uso de la información.

Las implicaciones de este tipo de incidentes pueden ser nefastas para una empresa o persona. Pues actualmente circula por la red, información absolutamente privada (como puede se lo concerniente al acceso de cuentas bancarias) que en caso de ser manipulada por personas no autorizadas, podría generar daños irreversibles.

Así bien, tanto a nivel internacional como nacional, se han consolidado una serie de normas que circunscriben este tipo de incidentes como delitos punibles y promueven la protección de la información, reiterando a las empresas y organizaciones la obligación que tienen, frente al manejo de los datos y la información. La implantación de un sistema de gestión de la seguridad de la información (SGSI) se convierte en un requisito indispensable de competitividad para todo tipo de empresa.

En este entendido, en la siguiente cartilla se desarrollará de manera general el marco normativo que regula la protección de la privacidad y el derecho a la intimidad en las relaciones laborales, se enunciarán algunos de los principales derechos individuales y fundamentales relacionados con las TIC y finalmente se hará énfasis en el marco normativo de protección de la información en Colombia.

U2 Metodología

La unidad está divida en cuatro temas, cada uno de las cuales cuenta con lecturas y documentales que ofrecen el aporte teórico correspondiente al mismo, acompañado de ejercicios de aplicación que facilitan el proceso de aprendizaje y algunos apartes de casuística.

Al final de la unidad el estudiante contará con los insumos esenciales para poder proteger y respetar lo expresado por la normatividad colombiana con respecto a la protección de datos, la privacidad y la intimidad.

U2

Desarrollo temático

La privacidad y el derecho a la intimidad

La privacidad y la intimidad son derechos fundamentales estipulados en el Artículo 15 de la Constitución Política colombiana, los cuales (señala la norma) deben ser respetados por el Estado y por quienes lo comprenden -Entidades públicas, privadas y personas naturales- esto, dado que son derechos personalísimos y fundamentales a los que se les debe una protección mucho más estricta, por emerger de la órbita íntima y exclusiva de cada persona.

Así bien, el derecho a la intimidad se desarrolla no solo a nivel nacional, sino también a nivel internacional, en un extenso número de instrumentos que instan su protección. Al respecto entonces, encontramos la Declaración Universal de Derechos Humanos (artículo 12), el Pacto Internacional de Derechos Civiles y Políticos (artículo 17.1), el Convenio para la protección de los Derechos Humanos y las libertades fundamentales (artículo 8.1) y el Pacto de San José de Costa Rica (artículo 11.2) que señalan que toda persona tiene derecho exclusivo sobre su vida privada y familiar, así como de su correspondencia y su domicilio, de esta manera, ninguna persona puede ser objeto de intromisiones abusivas en dichos escenarios.

Lo anterior es sencillo de advertir, cuando se enfrenta a un contexto privado como lo es el del domicilio y habitación de la persona, pues es claro que en este espacio el sujeto tiene pleno desarrollo de su privacidad e intimidad, al punto de que lo acontecido en dicha área queda indiscutiblemente excluido de la esfera pública. Ejemplo similar, el concerniente a los correos electrónicos o medios privados de comunicación (pensemos en Messenger, WhatsApp, Hotmail, Gmail, etc.) pues lo natural es pensar que existe un uso exclusivo de las cuentas por parte del titular.

No obstante, surge una dificultad en determinar los alcances del derecho a la intimidad y privacidad cuando se trata de espacios públicos, pensemos por ejemplo, en el sitio de trabajo o en redes sociales de libre acceso, pues incluso cuando el derecho a la intimidad y a la privacidad implica la no injerencia de los terceros en los espacios internos, propios, personales y exclusivos del individuo (Como lo ha sostenido la jurisprudencia de la Corte Constitucional colombiana), estos derechos no cuentan con un carácter absoluto e ilimitado, pues pueden ser interferidos siempre que exista un interés general, constitucional y prevalente que así lo exija.

En este sentido debemos preguntarnos: ¿Si los derechos a la intimidad y privacidad

permiten a su titular conminar a los que se inmiscuyan sin autorización, a los datos e información de este, ¿cuál es el límite de dicho derecho?

Pues bien, para lo anterior se hace necesario acudir a dos de los pronunciamientos más relevantes de la Corte Constitucional, pues es esta quien vela por la integridad y el respeto de los preceptos constitucionales:

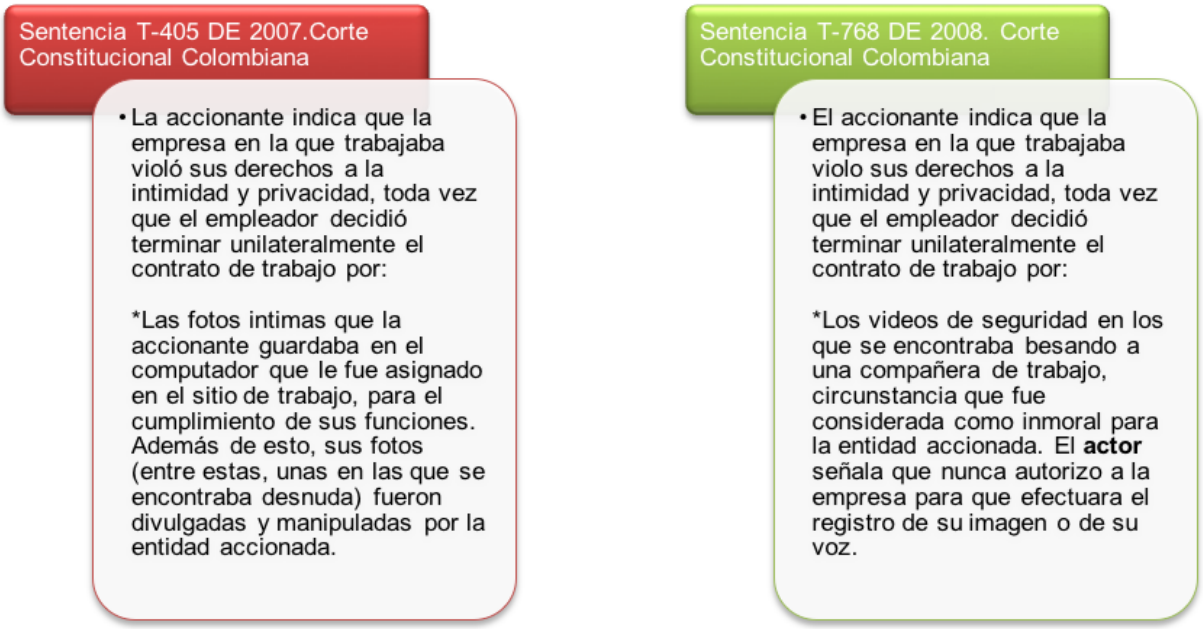


Figura 1
Fuente: propia

Frente al primer caso (Sentencia T-405 de 2007), La Corte Constitucional decide tutelar los derechos fundamentales a la intimidad, a la honra, al buen nombre, a la privacidad y a la autodeterminación sobre la propia imagen de la accionante e indica que el acceso a la información personal sin autorización de su titular, la divulgación del material encontrado y la manipulación del mismo son actitudes reprochables y por ende, deben ser sancionadas, decisión distinta la que toma en frente al segundo proceso (Sentencia T-768 de 2008) pues decide no tutelar lo indicado por el accionante, al señalar que no se encuentran vulnerados o amenazados ningún tipo de derechos.

Así bien, aunque en un inicio puedan parecer circunstancias similares, la Corte Constitucional pudo vislumbrar en las sentencias enunciadas, el punto de partida para determinar cuando los derechos a la privacidad e intimidad son vulnerados. Indica la Corte Constitucional, para los casos específicos, que el empleador puede tomar las medidas que considere necesarias, incluso cuando se limiten los derechos a la privaci-

dad e intimidad, al punto que el empleador puede implementar cámaras de videos y efectuar intromisiones legítimas, siempre que estas sean razonables, proporcionales y respeten la dignidad humana.

Claro, contrario sería pensar en las injerencias ilegítimas frente al derecho a la intimidad y privacidad que interesan única y exclusivamente al titular del derecho, en este sentido y por ejemplo, al tenor del Decreto 1543 de 1997 (artículo 35), el trabajador no cuenta con un deber legal de comunicar a su empleador afecciones de salud, como por ejemplo, ser portador del VIH, esto, por cuanto el aviso no es indispensable para la estabilidad y buen funcionamiento de la empresa. Así mismo, la instalación de cámaras de video en escenarios privados (vg. baños, instalaciones sindicales o lugares de servicios personales) es absolutamente reprochable, pues vulnera la dignidad, la privacidad y el derecho a la intimidad

En este sentido se insiste que la privacidad y el derecho a la intimidad pueden llegar a limitarse siempre que sea con fines legítimos (La seguridad y control de la empresa, por ejemplo), no vulnere la dignidad humana y resulte proporcional y razonable para el funcionamiento óptimo de la empresa, observando entonces con detenimiento, el objeto social de la misma (pues si es un banco requerirá más seguridad), el lugar donde se instaure la medida (Lugares públicos) y por último la finalidad, la proporcionalidad, los perjuicios, la publicidad y razonabilidad de la medida.

Figura 2
Fuente: propia

Se le recuerda al estudiante la importancia que implica conocer sus derechos fundamentales, pues de este depende la tutela oportuna de los mismos.

Principales derechos individuales y fundamentales relacionados con las TIC

Pensar en las TIC como un escenario apartado de los derechos que nos asisten como seres humanos, seria oprobioso en el Estado Social de Derecho que nos cobija y que ha sido promulgado por la constitución de 1991; En este entendido, es lógico pensar en las razones por las cuales desde el Estado Colombiano (a través de la Ley 1273 de 2009 y la Ley Estatutaria 1581 de 2012) hasta las Naciones Unidas (con la expedición de la Resolución de 1968) han promovido marcos legales para la protección de los derechos individuales y fundamentales que pueden llegar a vulnerarse con el uso de las TIC.Injurias, Calumnias, suplantación de identidad, hurtos, usos desfavorables de la información, atentados contra la confidencialidad, integridad y disponibilidad de la información, son delitos frecuentemente generados por el mal uso de las TIC, pues comprenden una violación directa a los derechos humanos y fundamentales, como lo son la intimidad personal, la intimidad familiar, el buen nombre (Art. 15 Constitución Política de Colombia), la honra (Art. 21 Constitución Política de Colombia), el derecho a la propia imagen (Derecho jurisprudencialmente constituido, vg. Sentencia T-634 de 2013), la libertad personal (Art. 13 y 20 Constitución Política de Colombia), el libre desarrollo de la personalidad (Art. 16 Constitución Política de Colombia), los derechos de los niños (Art. 44 Constitución Política de Colombia) y la Dignidad humana (Entendida esta, como principio rector), así como también derechos tales como el derechos de los consumidores, los derechos relativos a la propiedad intelectual , la protección de los trabajadores, la seguridad informática, entre otros.

Es importante resaltar que el acceso a las TIC es un derecho humano estipulado en la ley 1712 de 2014 (Articulo 4), norma que tiene como objeto regular el derecho y la garantía de acceso a la información pública, bajo los principios de la máxima publicidad para el titular universal, la transparencia, el acceso a la información pública, la no discriminación, la igualdad, entre otros.

Finalmente, y conforme a lo anterior, como medio de interacción social, las TIC deben fomentar la protección y prevalencia de los derechos del fuero interno, pues si bien, son un mecanismo de acceso a la cultura y educación, también pueden llegar a considerarse una amenaza potencialmente peligrosa.

La protección de datos en el Estado colombiano: Marco Normativo de Protección de la Información en Colombia

Para referirnos al marco normativo de protección de la información en Colombia, es importante anotar que incluso cuando la Ley Estatutaria 1582 de 2012 (y su Decreto reglamentario 1377 de 2013) es la norma en la que más se hace énfasis al momento de mencionar el tema en comento, existe previa y posteriormente a esta, una amalgama de normas que complementan la regulación efectiva de la protección integral de la información.

Así bien, cronológicamente podría señalarse que las normas más relevantes frente a la protección de la información en Colombia, son las siguientes:

Figura 3
Fuente: propia

Frente a la Ley 527 de 1999, cabe indicar que esta regula el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, así como también, instituye las entidades de certificación y hace mención a otras disposiciones de importancia. Para términos de estudio, se recomienda al estudiante leer el Artículo 2 de la norma, pues en esta se hace una descripción general de lo que significa un mensaje de datos, el comercio electrónico, la firma digital, el intercambio electrónico de datos, un sistema de información y una entidad de certificación. Así mismo, deben considerarse como criterios de interpretación de la ley (Articulo 3), el origen internacional, la uniformidad de aplicación y la observancia de la buena fe, entendida esta última como la exigencia que se hace a las personas naturales y jurídicas, de ajustar sus acciones conforme a la lealtad, honestidad y correcto comportamiento.

Ahora, conforme a la Ley Estatutaria 1266 de 2008 cabe señalar que esta se desarrolla bajo lo estipulado en los artículos 15 y 20 de la Constitución política, con relación a la protección de los datos y la información, así como también, al derecho fundamental del Habeas Data. En su Artículo 3, realiza una diferenciación adecuada entre Dato personal, Dato público, Dato semiprivado y Dato privado, enfatizando en el derecho que tienen todas las personas a conocer, actualizar y ratificar la información que sobre ellas se desprenda, tanto en el proceso de recolección y tratamiento, como en el proceso de circulación.

Cabe anotar que la Ley Estatutaria 1266 de 2008 señala en su Artículo 4 los principios de la administración de datos que deben considerarse siempre que se efectué una manipulación legitima de la información. Estos principios son el de veracidad de la información, el de finalidad legitima, el de la interpretación integral de los derechos constitucionales, el de confidencialidad, entre otros. Se recomienda al estudiante, hacer una lectura cuidadosa de estos.

Ahora, es la ley 1273 de 2009 de apenas cuatro artículos, la que modifica la Ley 599/00, es decir, el Código Penal Colombiano, instituyendo como un nuevo bien jurídico tutelado “la protección de la información y de

los datos". Establece la ley 1273 de 2009 nuevos delitos, de la siguiente manera:

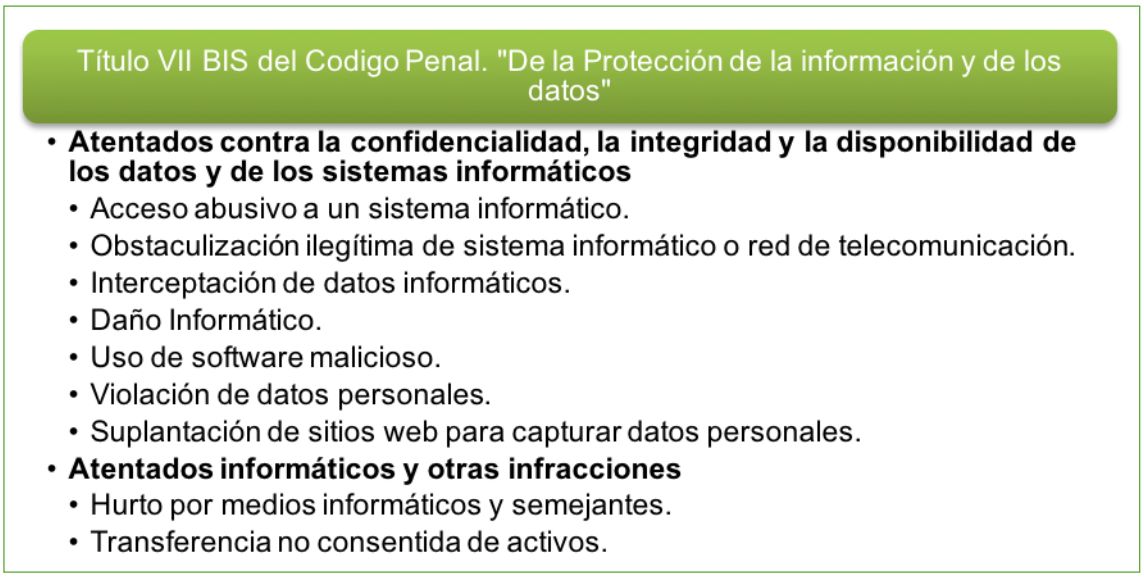


Figura 4
Fuente: propia

La ley establece para estos delitos, pena privativa de la libertad y multa. Frente a los Atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, se estipula prisión entre 48 y 96 meses y una multa de 100 a 1.000 SMLMV, excepto en el delito de Interceptación de datos informáticos, en donde se establece pena de prisión de 36 a 72 meses, en todos los casos, con posibilidad de agravación punitiva (Ver el Artículo 269H del Código Penal), con aumento de ½ a ¾ de la pena. Ahora, cuando se trata de hurto por medios informáticos y semejantes, la pena será análoga a la destinada para el hurto calificado del Art. 240 del Código Penal y, cuando se efectué transferencia no consentida de activos, la pena será de 48 a 120 meses de prisión y una multa de 200 a 1.500 SMLMV.

No obstante e incluso cuando existe un marco penal aplicable, el estudiante debe tener en cuenta que el proceso penal y su trámite desgastante, puede evitarse con la implementación adecuada de un sistema de gestión de la seguridad de la información (SGSI).

Ahora, conforme al Decreto 1727 de 2009, debe señalarse de manera general, que este configura un marco de partida, sobre la cual los operadores de los bancos de datos, deben hacer uso y presentación de la información (Según el Contrato efectuado), realizando la diferenciación entre la Información general del titular de la información, el Sector Financiero y el Sector Real.

Frente a la Ley Estatutaria 1581 de 2012, cabe decir que al igual que la Ley 1266 de

2008, regula el articulo 15 y 20 de la Constitución Política, pero esta se orienta únicamente a los datos personales (a diferencia de la Ley 1266 de 2008, que establece un marco normativo de los datos en general). La Ley Estatutaria 1581 de 2012, establece de manera complementaria, nuevos principios como el referente a la legalidad en materia de Tratamiento de datos, al Principio de libertad y el Principio de transparencia en el tratamiento de los datos personales.

Así mismo, la Ley Estatutaria 1581 de 2012 señala las excepciones a la prohibición del tratamiento de los datos sensibles (Artículo 6), entendidos estos como aquellos datos que pueden llegar a vulnerar la intimidad o derechos fundamentales del titular o generar una discriminación en contra de él. Se recomienda al estudiante efectuar una lectura reflexiva y consecuente de la ley en comento.

Frente a las actividades de inteligencia y contrainteligencia, la Ley Estatutaria 1621 de 2013, es la encargada de regular el manejo y manipulación de las bases de datos, estableciendo como principios, la necesidad (es decir, que la actividad sea menester para lograr los fines legal y constitucionalmente esperados), la idoneidad (deben usarse medios aptos e idóneos) y la proporcionalidad, e instituyendo como limitación de las actividades de inteligencia y contrainteligencia, las señaladas en el Artículo 4 de la Ley.

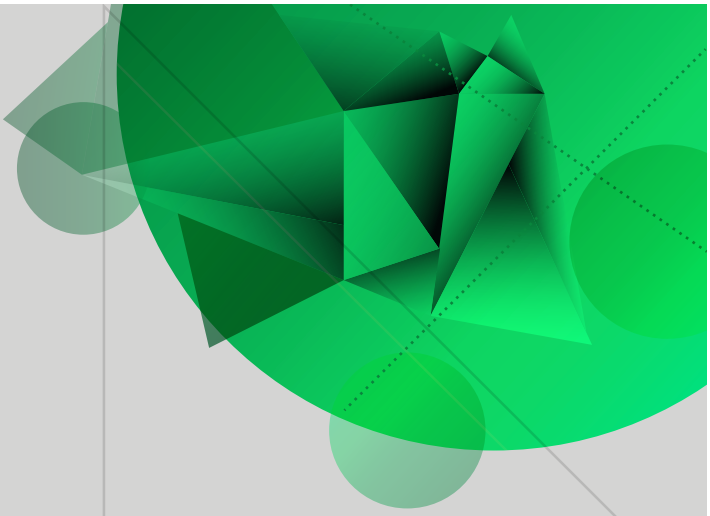
Por último, conforme a las normas más relevantes frente a la protección de la información en Colombia, debe mencionarse la Ley 1712 de 2014 o la "Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional", que señala que es publica la información se desprenda de los sujetos obligados, como son todas las entidad públicas, los órganos, organismos y entidades estatales, las personas naturales y jurídicas, públicas o privadas, que presten funciones o servicios públicos (Frente a la información relacionada directamente con la prestación de dicha función), entre otros (Ver Articulo 5 de la Ley 1712 de 2014), realizando la debidas excepciones en el Titulo III, del articulo 18 al 22. Es importante reiterar que la información debe ser divulgada al público por diversos medios, así como también debe otorgarse con función a derechos de petición de información y documentos que instaure cualquier persona, siempre que no se encuentre sujeto a las excepciones de publicidad.

Para finalizar, debe señalarse que la información es uno de los activos más importantes de una empresa y más significativos para las personas, bien sean jurídicas o naturales, en este entendido, su protección debe ser adecuada e idónea y debe en todos los casos, fundamentarse en el marco legal colombiano que tiene como fin la protección integral de la información, esto, con el propósito de evitar posibles procesos penales y amenazas o vulneraciones en el acceso y uso de la información. Recuerda que el Habeas data (El derecho a la intimidad, privacidad y protección de los datos) es un derecho fundamental, que se encuentra estipulado en el Artículo 15 de la Constitución Política, y por ende, siempre que se considere necesario, puede ser tutelado por medio de los diversos mecanismos de protección de derechos, como lo son el derecho de Petición, la Tutela o en última instancia, la denuncia.

3

Unidad 3

Metodologías de análisis de riesgo de la información



Sistema de Gestión de la Seguridad Informática

Autor: Ricardo López

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

Introducción

Siendo la información uno de los activos más importantes de las organizaciones, requiere medidas de protección y seguridad que permitan su disponibilidad, integridad y confiabilidad. Esa protección pasa, por realizar un análisis cuidadoso de los riesgos, amenazas y vulnerabilidades a las que está sometida.

El análisis del riesgo se asocia, en su forma más simple, al resultado que surge de la relación que se establece entre la amenaza y la vulnerabilidad de los elementos expuestos, con el fin de determinar los posibles efectos y consecuencias sociales y económicas asociadas a uno o varios fenómenos peligrosos en el ciberespacio y con referencia a la organización y cada una de sus dependendencias particulares.

Los cambios en uno o más de estos parámetros modifican el riesgo en sí mismo, es decir, el total de pérdidas esperadas y las consecuencias en un área determinada. El análisis de las amenazas y de las vulnerabilidades determina facetas del análisis del riesgo y debe estar articulados con este propósito y no comprender actividades separadas e independientes. Es decir, que un análisis de vulnerabilidad es imposible sin un análisis de amenazas y viceversa.

El riesgo describe la dimensión de los daños y las pérdidas que puede ocasionar un incidente. Se puede calcular como producto de los factores de amenaza y vulnerabilidad, en donde la primera toma en consideración las probabilidades de ocurrencia y las dimensiones del fenómeno, y la vulnerabilidad abarca los daños producidos por el fenómeno. La existencia de riesgo, y sus características particulares, se explica por la presencia de determinados factores, estos se clasifican, en general, en factores de amenaza y factores de vulnerabilidad.

Una “amenaza” se refiere al peligro latente que representa la probable ocurrencia o manifestación de un evento, que puede causar algún tipo de daño a la empresa y producir efectos adversos en las personas, la producción, la infraestructura y los bienes y servicios, es un factor de riesgo físico externo. Para su evaluación se deben adelantar inventarios con participación de las dependencias de la empresa, levantamientos y mediciones de campo y revisión de información con el fin de conocer la magnitud y severidad actual y potencial de los

eventos o fenómenos peligrosos. Como resultado de su estudio se obtienen los mapas de amenazas, instrumentos clave en la planificación del SGSI.

La "vulnerabilidad" se refiere a una serie de características diferenciadas de la empresa u organización, o subconjuntos de la misma, que la predisponen a sufrir daños frente al impacto de un evento externo, y que dificultan su posterior recuperación. Es sinónimo de debilidad o fragilidad, y la antítesis de capacidad y fortaleza, es un factor de riesgo interno.

En otras palabras, evaluar el riesgo es relacionar las amenazas y las vulnerabilidades en relación con la capacidad de respuesta o de autogestión de la organización que pueden dirigirse positivamente a la gestión de riesgo:

$$\text{RIESGO} = \frac{\text{Amenaza X Vulnerabilidad}}{\text{Capacidad de reacción}}$$

El riesgo y la vulnerabilidad preexistentes se expresan de forma indiscutible en la manifiesta búsqueda de una estrategia de desarrollo basada en procesos que implican como componente fundamental, la reducción de la vulnerabilidad existente.

En este módulo, estudiaremos las definiciones y conceptos relevantes así como la clasificación de los mismos. Continuaremos con el ejercicio de la unidad 3, con el fin de completar el diagrama para la implantación del SGSI desarrollado por el "Foro de implementación ISO 27K" aplicado a su empresa (real o ficticia) con la que ha desarrollado la asignatura.

U3

Metodología

La unidad está divida en 2 temas, cada uno de los cuales cuenta con lecturas y documentales que ofrecen el aporte teórico correspondiente al tema, acompañado de ejercicios de aplicación que facilitan el proceso de aprendizaje. Dichos ejercicios requieren que el estudiante, cuente con la documentación de una empresa (real o ficticia) sobre la cual aplicará los conceptos aprendidos.

Al final de la unidad tendrá los insumos iniciales para consolidar un ejercicio de evaluación en la gestión de seguridad de la información de dicha empresa y esta se constituirá junto al test final en su nota de módulo.

En esta semana se iniciará la participación en el Foro donde se socializará su producción académica durante el modulo.

Metodologías de análisis de riesgo de la información

La construcción de una guía de Gestión del Riesgo para la organización se estructura en 6 pilares a saber: Establecimiento del contexto – evaluación del riesgo – tratamiento del riesgo – aceptación del riesgo – comunicación del riesgo – monitoreo y revisión del riesgo.

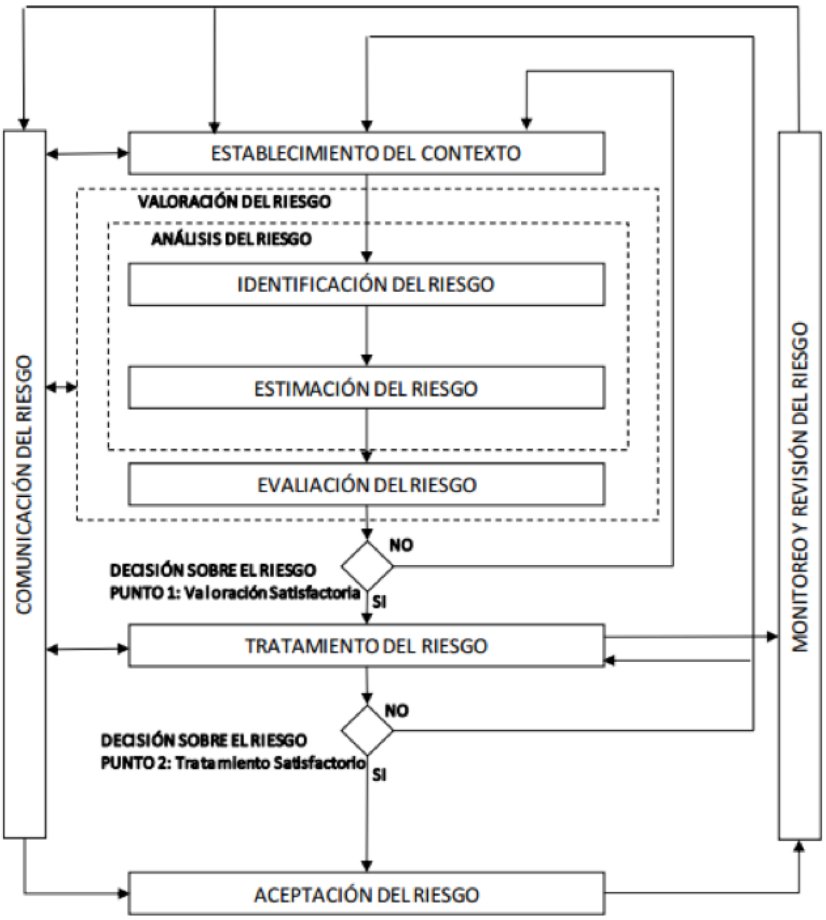


Figura 1
Fuente: NTC-ISOMEC 27005

Proceso de SGSI	Proceso de gestión del riesgo
Planificar	Establecer el contexto. Valoración del riesgo. Planificación del tratamiento del riesgo. Aceptación del riesgo.
Hacer	Implementación del plan de tratamiento de riesgos.
Verificar	Monitoreo y revisión continuos de los riesgos.
Actuar	Mantener y mejorar el proceso de gestión del riesgo en seguridad de la información.

Tabla 1. Alineamiento del SGSI y la gestión del riesgo
Fuente: propia, basada en la NTC ISO/ICE 27005

Establecimiento del contexto: Implica establecer

- Criterios básicos necesarios para la gestión del riesgo: criterios de evaluación, de impacto y de aceptación del riesgo.
- Definir los alcances y límites: garantizar que todos los activos se tomen en consideración, de acuerdo a su relevancia y jerarquización de importancia.
- Establecer una organización adecuada que opere la GR: identificar las dependencias involucradas, asignarles funciones y responsabilidades y establecer una ruta para escalar decisiones y especificar los registros que se deben conservar.

Valoración del riesgo: implica la identificación y descripción cuantitativa y cualitativa del riesgo lo que permite priorizar frente a los criterios de evaluación del riesgo establecidos para la organización.

- Identificación del riesgo: permite inferir por una perdida potencial y como y donde podría generarse esta perdida.
- Identificación de los activos: relaciona la cantidad de activos y su relevancia, así como el propietario o responsable del mismo.
- Identificación de las amenazas: buscar información sobre las amenazas y sus orígenes. Generar una línea de tiempo de exposición al riesgo y a sus transformaciones tecnológicas.

D= Deliberadas A= Accidentales E=Ambientales

TIPO	AMENAZA	ORIGEN
Daño físico	Fuego	A, D, E
	Agua	A, D, E
	Contaminación	A, D, E
	Accidente Importante	A, D, E
	Destrucción del equipo o medios	A, D, E
	Polvo, corrosión, congelamiento	A, D, E
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fenómenos volcánicos	E
	Fenómenos meteorológico	E
	Inundación	E
Perdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado	E
	Perdida de suministro de energía	E
	Falla en equipo de telecomunicaciones	
Perturbación debida a la radiación	Radiación electromagnética	
	Radiación térmica	
	Impulsos electromagnéticos	
Compromiso de la información	Interceptación de señales de interferencia comprometida	
	Espionaje remoto	
	Escucha encubierta	
	Hurto de medios o documentos	
	Hurto de equipo	
	Recuperación de medios reciclados o desechados	
	Divulgación	
	Datos provenientes de fuentes no confiables	
	Manipulación con hardware	
	Manipulación con software	
	Detección de la posición	
Fallas técnicas	Fallas del equipo	
	Mal funcionamiento del equipo	
	Saturación del sistema de información	
	Mal funcionamiento del software	
	Incumplimiento en el mantenimiento del sistema de información.	

Figura 2
Fuente: http://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

- Identificación de los controles existentes: realizar un inventario de los controles implementados en la organización, evaluando su funcionamiento y su efecto para reducir la vulnerabilidad. Revisando los documentos que lo sustentan, verificando con el personal que lo maneja y verificando la estructura física relacionada.
- Identificación de las vulnerabilidades: relacionar las amenazas con los riesgos para determinar la vulnerabilidad. Debe identificarse en cada una de las dependencias de la organización y en cada uno de los pasos de los procesos de gestión.
- Identificación de las consecuencias: identifica los daños que podrían ser causados por un escenario de incidente.

Metodologías para la estimación del riesgo

Estimación cualitativa	Escala de atributos calificativos para describir la magnitud de las consecuencias potenciales.
Estimación cuantitativa	Escala con valores numéricos a partir de información de diferentes fuentes.

Tabla 2
Fuente: propia

Evaluación de las consecuencias del riesgo

Lista de escenarios de incidentes				
identificación de amenazas	vulnerabilidades	activos afectados	consecuencias para los activos	procesos del negocio

Tabla 3
Fuente: propia

Evaluación de la probabilidad de incidentes

Lista de escenarios de incidentes							
identificación de amenazas	vulnerabilidades	activos afectados	consecuencias para los activos	procesos del negocio	controles existentes y planificados	Eficacia e implementación	estado de utilización

Tabla 4
Fuente: propia

Tratamiento de riesgos. Sistema de gestión de seguridad de la información

Frente a los riesgos clasificados y evaluados en una organización, existen cuatro alternativas posibles a seguir:

Reducción del riesgo	Retención del riesgo	Evitación del riesgo	Transferencia del riesgo
• Mediante la seleción de cntroles adecuados y justificados • Criterios de aceptación del riesgo, requisitos legales, reglamentarios y contractuales	• Desición de no implementar controles sobre un riesgo pues se puede retener	• Desición para evitar por completo el riesgo, mediante el retiro de una actividad existente o planificada.	• Desición de compartir el riesgo con partes externas. Se puede transferir el riesgo pero no el impacto.

Figura 4
Fuente: propia

La ruta del tratamiento de riesgos, según ISO 279005, se describe en este diagrama consignado en la norma:

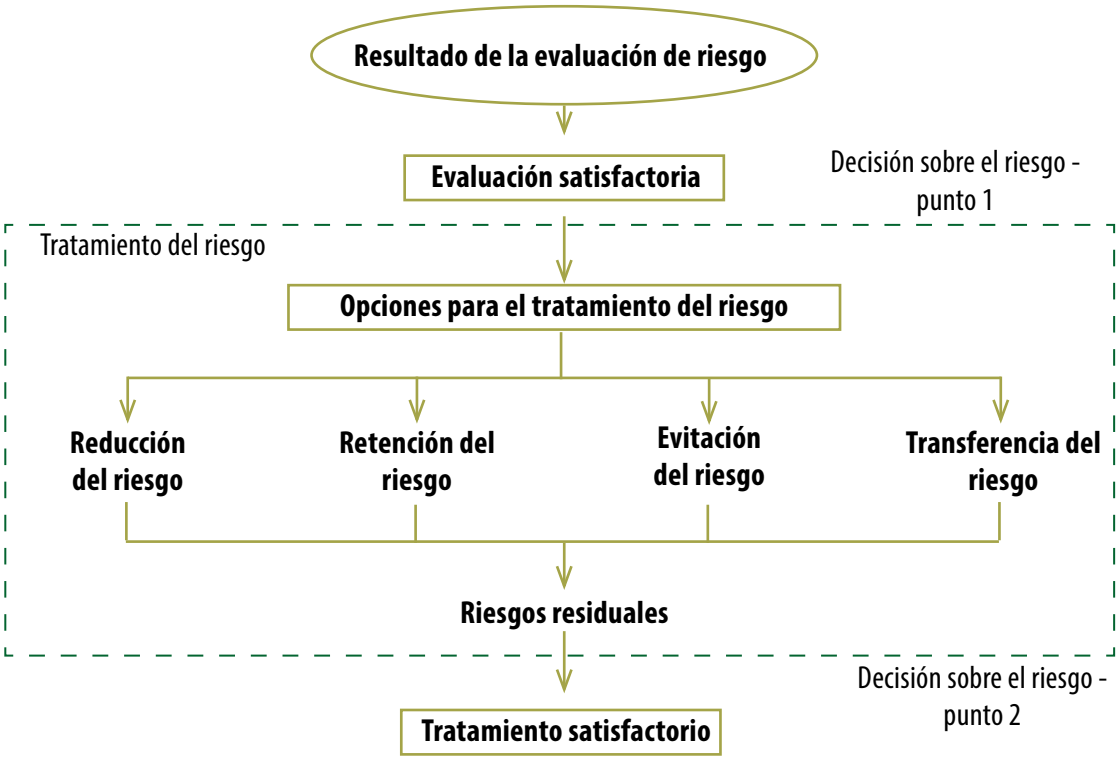


Figura 5
Fuente: propia

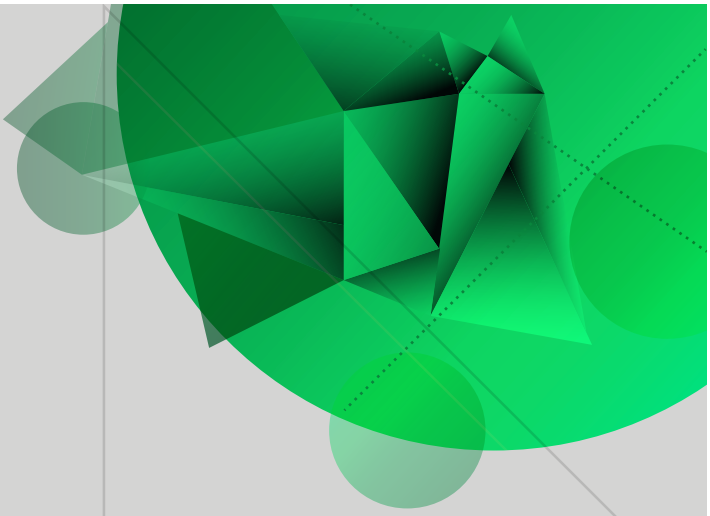
La implementación del tratamiento de riesgos, busca disminuir al máximo las consecuencias adversas de los riesgos, con una inversión razonable y mínima en recurso humano y económico, lo que se logra a través de la planificación de una guía de gestión de riesgos que contemple, en este apartado específico de aceptación los siguientes elementos:

- Criterios del negocio.
- Aspectos legales y reglamentarios.
- Operaciones.
- Tecnología.
- Finanzas.
- Factores sociales y humanitarios.

3

Unidad 3

Gestión de incidentes



Sistema de Gestión de la Seguridad Informática

Autor: Ricardo López

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

Introducción

En la actualidad es común escuchar testimonio de personas que han sufrido problemas en sus sistemas de información, fallos, incidentes de IT, que de alguna manera han afectado el trabajo de las empresas, acciones como borrado accidental de data, alteración, modificación, acceso no autorizado, robo o pérdida de información valiosa y relevante para la empresa, por otra parte afección por desastres naturales, fallos de energía, huracanes, terremoto, entre otros afectaran el buen desarrollo de las actividades empresariales, el gran reto para nosotros los ingenieros IT es prepararnos en el desarrollo de planes y/o accionen tendientes a minimizar las afecciones generadas por un incidente, fallo o desastre.

En este capítulo trabajaremos la definición, clasificación, análisis, tratamiento, resolución y cierre de incidente de seguridad en ambientes IT.

U3 Metodología

La unidad está divida en cuatro temas, cada uno de las cuales cuenta con lecturas y documentales que ofrecen el aporte teórico correspondiente al mismo, acompañado de ejercicios de aplicación que facilitan el proceso de aprendizaje y algunos apartes de casuística.

Al final de la unidad el estudiante contara con los insumos esenciales para poder Definir, clasificar, analizar, tratar, resolver y dar cierre a incidentes de seguridad.

Componente motivacional

Frente a la gestión de Incidentes IT en Colombia, ¿Conoce usted el tratamiento que las empresas públicas y privadas realizan frente a un incidente IT?, ¿Sabe usted quien o quienes son los encargado(s) de la gestión de incidentes IT en su empresa? ¿Sabe usted que tipos de incidentes se pueden presentar en la empresa y cómo afrontarlos?,¿Está preparado usted y su empresa para afrontar incidentes IT?

U3

Desarrollo temático

Gestión de incidentes

Se define un incidente como un evento no esperado que causa la interrupción del servicio de software, hardware, acceso, extracción de datos, entre otros.

Al presentar muchos incidentes se deben establecer prioridades basados en el impacto del negocio, la determinación del impacto dependerá de la urgencia e impacto que se tiene en la empresa, se debe estimar el personal, los recursos, y el tiempo para resolver el incidente.

Si no se puede resolver es necesario escalar a instancias superiores que permita resolver el incidente presentado brindando solución al usuario.

Existe un escalamiento funcional el cual es horizontal y requiere de más personas con más privilegios, también existe el escalamiento jerárquico que consiste en escalar verticalmente el incidente a una persona con mayor autoridad dentro del proceso IT.

El Objetivos de Gestión de incidentes es resolver los incidentes y restituir el servicio con un menor impacto, teniendo un enfoque estructurado y bien planificado, obteniendo como resultado mayor resolución de incidentes en el menor tiempo de respuesta, mayor productividad, monitoreo de eventos, uso eficaz del personal y mejor respuesta y servicios al usuario final.

La Gestión de Problemas no se debe confundir con la gestión de incidentes (aunque existe una estrecha relación) ya que la gestión del problema se orienta a encontrar y analizar las causas a un determinado incidente y la gestión de incidentes a restablecer el servicio.

Propiedades y funcionalidades de Gestión de Incidentes

Pasos y acciones a desarrollar en cada etapa del proceso

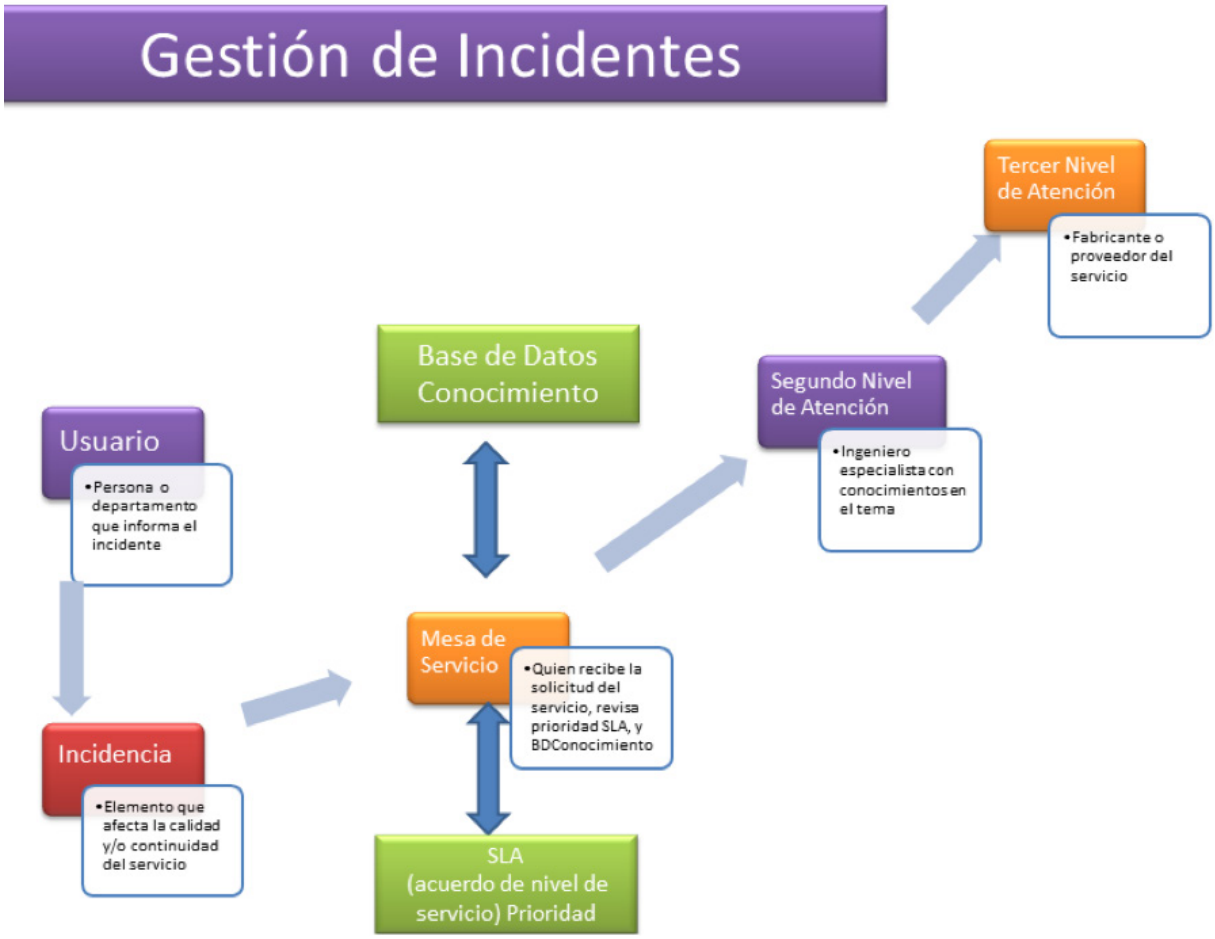


Imagen 1
Fuente: Propia.

Definición por proceso

1. Usuario: persona y/o departamento que reporta el incidente.
2. Incidencia: interrupción de un servicio, aplicación o recurso, informada por un usuario o generada por una aplicación.
3. Service Desk - Help Desk: es la primera línea de soporte, responsable de la gestión de la incidencia. Es quien recibe la solicitud del servicio, clasifica la prioridad del incidente mediante SLA (acuerdos de nivel de servicio), revisa la base de datos del conocimiento y trata de dar solución y/o restablecer el servicio. De no poseer el conocimiento y/o dar solución al incidente escalará a soporte de segundo nivel si este no tiene la solución pasara a soporte de tercer nivel (Proveedor y/o fabricante).
    - SLA Registro y clasificación del incidente: se genera el registro del incidente, se determina la prioridad mediante la ecuación Prioridad= Impacto*Urgencia; seguidamente se categoriza asignado personal de soporte especialista en ese tipo de incidente.
    - KBD: bases de datos de conocimiento Análisis y diagnóstico.
    - Resuelto: si se conoce el método de solución asignar los recursos necesarios; si No se conoce el método de solución se escala a nivel superior de soporte.
    - Si es Escalado se debe escalar hasta encontrar la solución: existen dos tipos de escalado.
    - Escalado Funcional requiere de más personas con más privilegios y/o personal especializado o de nivel superior.
    - Escalado Jerárquico escalar a personal con más autoridad dentro del proceso, incluso entes externos o proveedores.
    - Una vez solucionado el incidente continuar con el cierre.
4. Resolución y cierre: una vez solucionado el incidente proceder a documentar y registrar en el sistema o en la base de datos de conocimiento la solución planteada. De ser necesario generar un RFC (petición de cambio) a la gestión de cambio.
5. Monitorización y seguimiento: el proceso debe ser controlado mediante emisión de informes, actualización de bases de datos, y monitorización de los niveles de servicios.

Es importante que exista una relación entre la gestión de incidentes y otros procesos de IT como gestión de problemas, gestión de cambios, gestión de disponibilidad, gestión de servicios, entre otros.

Nivel de prioridad:

El ministerio de TIC en el documento "Guía para la gestión y clasificación de incidentes de seguridad", define que el nivel de prioridad de un incidente Depende del valor o importancia dentro de la entidad y del proceso que soporta el o los sistemas afectados.

Nivel Criticidad	Valor	Definición
Inferior	0,10	Sistemas no críticos, como estaciones de trabajo de usuarios con funciones no críticas.
Bajo	0,25	Sistemas que apoyan a una sola dependencia o proceso de una entidad.
Medio	0,50	Sistemas que apoyan más de una dependencias o proceso de la entidad.
Alto	0,75	Sistemas pertenecientes al área de Tecnología y estaciones de trabajo de usuarios con funciones críticas.
Superior	1,00	Sistemas Críticos.

Imagen 2
Fuente: http://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

Tiempo de respuesta

MINTIC en la cartilla 21 ha establecido tiempos máximos de respuesta para la atención de incidentes de seguridad y atención de los mismos, de acuerdo a su criticidad e impacto. Los tiempos expresados en la siguiente Tabla son un acercamiento al tiempo máximo en que el incidente debe ser atendido, y no al tiempo en el cual el incidente debe ser solucionado.

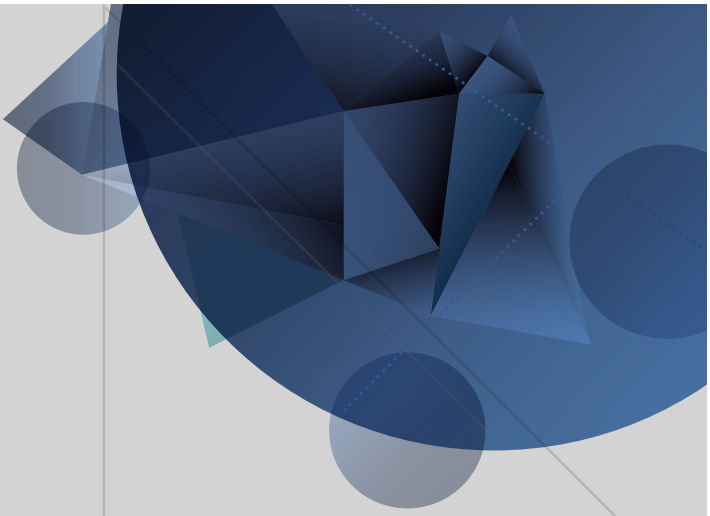
Nivel Prioridad	Tiempo de Respuesta
Inferior	3 horas
Bajo	1 hora
Medio	30 min
Alto	15 min
Superior	5 min

Imagen 3
Fuente: http://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

4

Unidad 4

Gestión del negocio



Sistema de Gestión de la Seguridad Informática

Autor: Ricardo López

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

Introducción

La importancia de la gestión del negocio radica en la continuidad del mismo, ya que de no poder atender incidentes que impliquen o atenten contra los servicios ofrecidos por el negocio, este tendera a perder competitividad en el mercado y de no tener un plan apropiado de continuidad puede llegar hasta el cierre del mismo.

El objetivo del departamento TI en la gestión del negocio, es aportar el mayor valor a la empresa, optimizando recursos (humanaos, financieros, tecnológicos, materiales), generando planes de continuidad del negocio, mejorando el servicio prestado, apoyando a otros departamentos, optimizando los procesos del negocio, la comunicación y aplicando las mejores prácticas, asegurando que los recursos asociados sean utilizados correctamente y generen valor para el negocio.

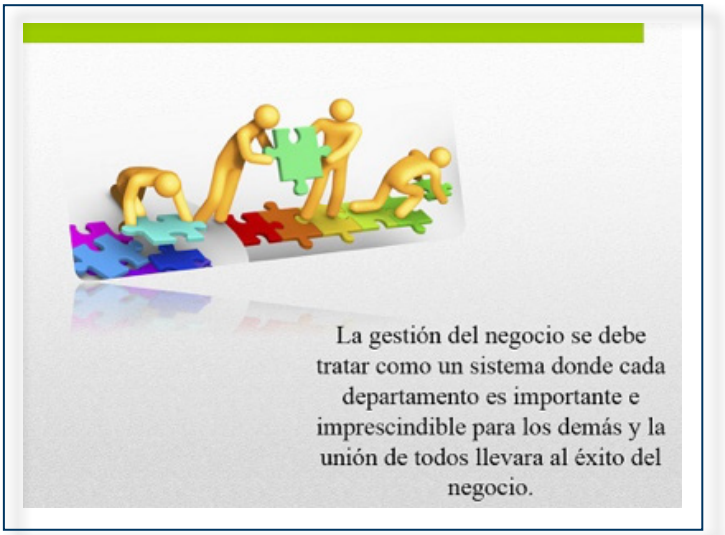


Figura 1
Fuente: propia

U4 Metodología

La unidad está divida en seis temas, cada uno de las cuales cuenta con lecturas y documentales que ofrecen el aporte teórico correspondiente al mismo, acompañado de ejercicios de aplicación que facilitan el proceso de aprendizaje y algunos apartes de casuística.

Al final de la unidad el estudiante contara con los insumos esenciales para poder definir los componentes del negocio, los diversos tipos de desastres a los que se ven enfrentadas las empresas, generar estrategias de mitigación y plan de continuidad del negocio.

U4

Desarrollo temático

Gestión del negocio

Hablar de gestión del negocio es hablar de la adecuada administración y optimización de procesos y recursos en la organización asegurando que los recursos asociados sean utilizados correctamente y generen valor para el negocio.

El negocio de una empresa depende en gran parte de la información y los sistemas que la soportan, esto hace imprescindible que el departamento de TI se alinee con los objetivos del negocio y con las necesidades de los usuarios, cambiando la visión del departamento de TI de administradores de tecnología a administradores de servicios de TI. Con esto NO quiero indicar que se deben dejar de lado la infraestructura, los servidores, las redes, el software, sino al contrario estos elementos utilizarlos como herramienta que optimicen la calidad del servicio requerido por el usuario y que apalanquen el objetivo del negocio.

Al usuario no le interesa saber si el proxy funciona, como funciona, deja de funcionar, el solo quiere conectividad rápida, acceso a los sitios y recursos que necesita para desarrollar su labor es decir "un buen servicio", para esto es necesario desarrollar el plan de negocio el cual debe contener al menos, un perfil de la empresa, un plan de mercadeo, un plan de operaciones un plan de recursos humanos y financieros, un plan de gestión de recursos tecnológicos dentro el cual se debe incluir un plan de continuidad del negocio, todos alineados y apuntando a conseguir el objetivo del negocio.

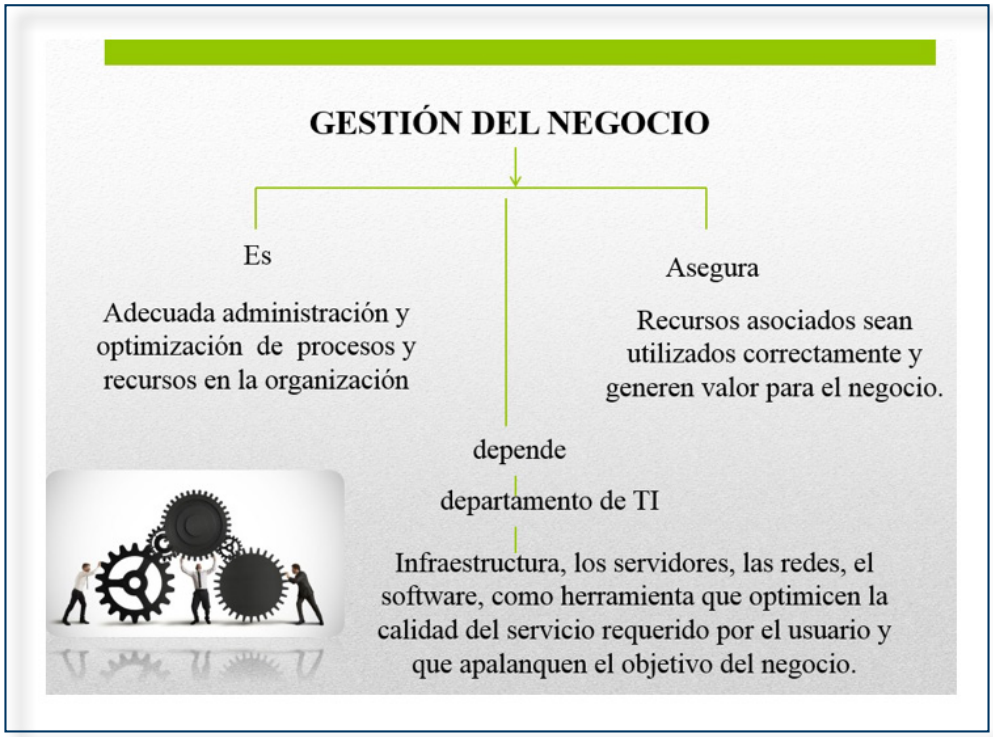


Figura 2
Fuente: propia

La gestión del negocio se debe tratar como un sistema donde cada departamento es importante e imprescindible para los demás y la unión de todos llevara al éxito del negocio.

Existen modelos internacionales para las diversas áreas de gestión TI entre los cuales se destacan:

ITIL: (IT Infrastructure Library, biblioteca de infraestructura de TI), el cual es un marco de referencia de mejores prácticas para la administración de servicios de TI.

COBIT: (Control Objectives for Information Systems and related Technology) modelo de referencia para desarrollo de proyectos de gobierno TI y auditoria.

PMI: (Project Management Institute) Modelo para la administración y gestión de proyectos TI.

Tipos de desastres a considerar

Desastres Naturales considerados como eventos inesperados causados por la naturaleza y que pueden llegar a interrumpir el servicio ofrecido por la compañía (terremotos, huracanes, inundaciones, incendios, entre otros).

Desastre Antropogénicos o provocados por el hombre, estos pueden ser por error o con intención de causar daño, pero afectaran la gestión de servicios de la compañía (borrado de información, sustracción, perdida, manipulación de información, robo de

dispositivos o equipos, daño en infraestructura, entre otros).

Sinérgicos los cuales surgen de la interacción entre desastres naturales y provocados por el hombre.

Realidad TI en la empresa

La tecnología ayuda a la organización a ser diferente, quien mejor use la tecnología tendrá mayores ventajas, va a llegar primero, ofrecerá un servicio más rápido y de mejor calidad, reducirá costos, generara una comunicación más efectiva y eficiente.

Pero en la actualidad, ¿qué esperan las organizaciones del departamento de tecnología?, se tiende a pensar que el departamento TI debe crear tecnología y en parte es cierto, pero no puede limitarse a generar conexiones, instalar equipos, utilizar diversos programas y herramientas, desarrollar software por desarrollar, configurar servidores. El verdadero objetivo del departamento de TI debe ser apoyar y potenciar los objetivos de la organización es decir apuntar al cumplimiento de los objetivos capacitando al personal para el logro de los mismos, orientando el desarrollo al cumplimiento de las metas de la compañía, evidentemente tener una excelente base de datos, la mejor conectividad, los mejores canales de comunicación, equipos de última tecnología, servidores veloces y con amplia capacidad del almacenamiento, almacenamiento en la nube, entre otros obviamente generaran beneficios a la compañía.

Figura 3
Fuente: propia

Es por esto que debemos realizarnos cada periodo esta pregunta ¿qué proyectos propongo a corto plazo que apunten a apoyar y potenciar los objetivos de la organización? Potenciar personas, departamentos, unidades para alcanzar los logros, o simplemente crear tecnología porque puedo, conozco y manejo la tecnología, pero ojo eso no busca la organización.

Es importante que el departamento de TI mantenga una comunicación fluida y asertiva con todas las áreas del negocio (utilizando un lenguaje claro, entendible, no técnico), en especial la gerencia, ya que es común que la gerencia no comunique los objetivos de la empresa o estos no sean claros para los diferentes departamentos y si no hay claridad no se articulan las diversas áreas para la consecución de dichos objetivos.

Es común que la gerencia del negocio toma decisiones sin contar con el departamento de TI y esperan magia del departamento de TI todo lo piden para ya.

¿Qué quiere la organización?

Generalmente la tecnología y el negocio están separados es decir no apuntan al mismo objetivo. La tecnología es parte del negocio y al negocio no le gusta que la tecnología cueste ya que cualquier proyecto de tecnología requiere altas inversiones de dinero. El negocio quiere respuestas inmediatas pues piensa que la tecnología solo es enchufar y listo, pero no es así los proyectos TI requieren de tiempo, de planeación, de pruebas, de ejecución, de seguimiento, para poder entregar unos óptimos resultados. De aquí se hace indispensable la correcta venta del proyecto TI, al hablar de costos resaltar los beneficios que el proyecto traerá y la pronta recuperación de la inversión. Al hablar de tiempos resaltar la vida útil y el aporte del proyecto a la consecución de los objetivos del negocio.

Principales errores en los que Gestión de TI cae y por los cuales pierden credibilidad los proyectos TI

1. Implementar y/o proporcionar soluciones que no se usa, lo más común portales y aplicaciones.
2. Proporcionar soluciones que llegan tarde, ejemplo: desarrollar una aplicación por 6 meses y cuando la terminan ya tienen otra solución implementada. Esto genera frustración y cuestionamiento del departamento de TI por parte del negocio. ¿a qué se dedican los de tecnología?
3. Otro error común es no medir el impacto de la tecnología, o Invertir en tecnología que no impacta al cliente final.
4. Proponer soluciones que no encajan.
5. Pedir presupuesto y no mostrar resultados. El negocio suele pensar que TI pide y pide recurso y no generan resultados ni beneficios.
6. La comunicación entre TI y el negocio es inoperante por el lenguaje técnico que se utiliza. (Es importante que se hable el mismo lenguaje).

ITIL

ITIL (information Technologie infraestructure library) es una biblioteca que contiene las buenas prácticas para la gestión de los servicios de TI, no es un método, tiene 3 principios, procesos, calidad y clientes. Propone soluciones a problemas pensando en el cliente.

ITIL pretende que la tecnología se mueva, alinee e integre con el negocio, ITIL parte desde el área de tecnología, y es un grupo de buenas prácticas para la gestión del negocio.

Su primera publicación es en 1989 por CCTA (Central Computer Telecomunications Agency) para el gobierno del reino unido 52 libros.

En el año 2000 se realiza una revisión y se resumen en 7 libros, llamado ITIL versión 2.

En el año 2007 se publica ITIL versión 3.

En el año 2011 se genera la versión que en la actualidad se utiliza, se alinea al ciclo de vida de los servicios y se recogen buenas prácticas para las organizaciones. ITSMF (foro para la gestión de los servicios).

Los 5 libros propuestos en ITIL para consolidar el modelo de Ciclo de Vida del Servicios son:

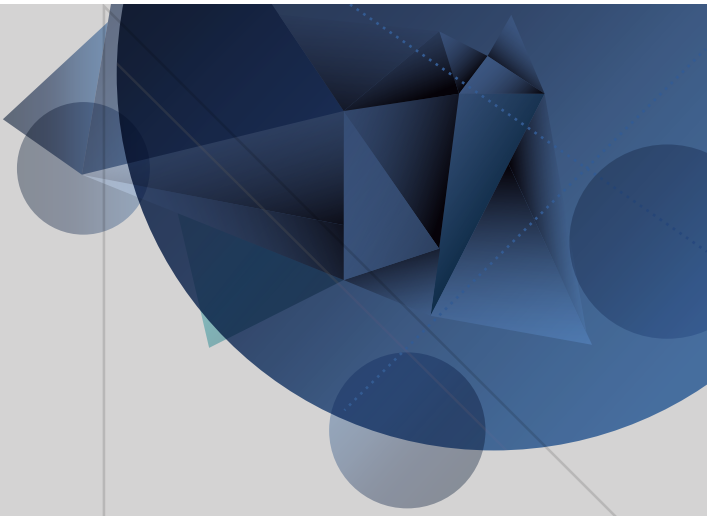
1. Estrategia del servicio: el centro del Ciclo de Vida del Servicio. Promueve la visión de la gestión del servicio como un activo estratégico, y no solo como una capacidad de la organización. En esta etapa se deben identificar las oportunidades de negocio, definir los servicios a implementar (menú de servicios) y el porqué, estudios económicos y de factibilidad, generar la identidad del negocio y las estrategias del mismo, también asignar actividad, procedimiento y rol. Es decir asignar tareas, procesos a personas y/o departamentos. Se asocia a la gestión financiera, gestión de portafolio de servicios, gestión de demanda.
2. Diseño del servicio: los principios de diseño y los métodos necesarios para convertir los objetivos de negocio estratégicos en un catálogo de servicios con sus activos asociados, el principal objetivo es diseñar los servicios nuevos o modificados, de forma alineada con los objetivos de negocio establecidos en la Estrategia del Servicio, para incorporarlos al Catálogo de Servicios e implantarlos posteriormente en producción. Se asocia a la gestión de continuidad, gestión de servicio, gestión de disponibilidad, gestión catálogo de servicios.
3. Transición de servicios: el objetivo es la implantación de los Servicios nuevos o modificados con el mínimo impacto para el negocio y dentro de los parámetros previstos de coste, tiempo y calidad. Se asocia con la planificación, gestión de cambios, gestión de configuración, gestión del conocimiento, validación y pruebas de servicio.
4. Operación del servicio: en esta etapa los servicios aportan valor al negocio y los planes, diseños y mejoras del Ciclo de Vida del Servicio son ejecutados y evaluados, se realizan todas las actividades necesarias para la prestación y el soporte de los servicios. Se asocia la gestión de eventos, gestión de incidentes, gestión de problemas, gestión de peticiones, gestión de servicios, gestión de operaciones, service desk, gestión de aplicaciones.
5. Mejora continua del servicio: alinear y realinear los servicios con las necesidades cambiantes de negocio identificando e implementando mejoras. Todas las fases son susceptibles de mejora tanto la estrategia, como el diseño, como la transición, como la operación de los servicio. Como todo proceso de mejora continua aplica el Ciclo de Deming

PDCA: Planificar (Plan), Hacer (Do), Verificar (Check) y Actuar (Act). Se asocia al proceso de mejora, e informe de servicios.

4

Unidad 4

ISO/FDIS 22301: 2012 Seguridad De La Sociedad – Sistema De Gestión De La Continuidad De Los Negocios SGCN/BCMC



Sistema de Gestión de la Seguridad Informática

Autor: Ricardo López

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

Introducción

La exposición al riesgo es una realidad en toda empresa, existen multitud de amenazas que atentan y afectan la información (incendios, terremotos, inundaciones, fallos eléctricos, malware, hurtos, espionaje, hacking, entre otros), esta afección a la información y los sistemas que la soportan afectaran directamente al negocio y de no contar con un plan de continuidad adecuado podrá llegar hasta el cierre del mismo.

En latino América especialmente en Colombia existe la mentalidad orientada a solucionar problemas e incidentes de último minuto gracias a nuestra creatividad, pero NO podemos permitir que el destino de la empresa dependa de la suerte o creatividad del TI del momento. Es por ello que se hace imprescindible desarrollar estrategias orientadas a la mitigación de riesgos y eventos que atenten contra la continuidad del negocio.

Las empresas deben estar preparadas para que un evento fortuito no acabe con ellas, el punto de partida será el desarrollo de un análisis y evaluación de riesgo de interrupción o continuidad, que contemple las probabilidades de ocurrencia de un evento y el análisis de cuales actividades son críticas para la compañía al igual que la estimación del tiempo de recuperación ante determinado incidente.

Por otra parte es importante tener claro que ningún mapa de riesgos por muy bien desarrollado que este, va dejar ver todos los riesgos a los que está expuesta la empresa. Por este motivo se hace imprescindible contar con un comité de manejo de crisis el cual debe estar conformado por personal preparado y capacitado en protocolos y herramientas para toma de decisiones en eventos que están fuera de control.

U4 Metodología

La unidad está divida en seis temas, cada uno de las cuales cuenta con lecturas y documentales que ofrecen el aporte teórico correspondiente al mismo, acompañado de ejercicios de aplicación que facilitan el proceso de aprendizaje y algunos apartes de casuística.

Al final de la unidad el estudiante contara con los insumos esenciales para poder desarrollar un mapa de análisis de riesgos de interrupción y/o continuidad del negocio y tomar las medidas necesarias para contrarrestar cualquier incidencia, estando en capacidad de generar un plan de continuidad del negocio.

ISO/FDIS 22301: 2012 Seguridad De La Sociedad – Sistema De Gestión De La Continuidad De Los Negocios SGCN/BCMC

La norma ISO 22301:2012 SGCN establece los requisitos para planificar, establecer, implementar, operar, monitorear, revisar, mantener y mejorar continuamente un sistema de gestión documentado para prepararse, responder y recuperarse de eventos perturbadores que puedan surgir, asegura la continuidad y busca la certificación internacional de buenas prácticas de gestión de la continuidad del negocio.

La ISO define esta norma como "Proceso de gestión que provee un marco conceptual para crear o salvaguardar a los objetivos de la organización incluyendo sus obligaciones" (ISO/FDIS 22301:2012).

El sistema de gestión de la continuidad hace parte del sistema Gestión, La norma ISO22301 hace mayor énfasis en el objetivo real, el liderazgo, las métricas, la medición de desempeño, el estado inicial y el estado ideal

Esta es una norma certificable, sus requisitos son genéricos y aplicables a cualquier tipo de organización. Complemento de esta norma existe la norma ISO 22300 (no certificable) la cual define el vocabulario, la norma ISO 22313(no certificable) la cual es el código de buenas prácticas para alcanzar la certificación en ISO 22301, estas normas se basan y apoyan en las normas británicas BS2599-1 buenas prácticas y BS2599-2 certificable.

La gestión de continuidad del negocio genera grandes y variados beneficios a la compañía entre los que se destacan, generar una respuesta eficaz ante una crisis o incidente, protección de las personas, reputación y buen nombre de la empresa o marca, una mejor comprensión de la organización, reducción de costos, confianza de los clientes, preserva el interés de los accionistas, mayor competitividad, mayor eficacia operativa, cumplimiento de las normas, mantenimiento unidades claves del negocio, cumplimiento de la ley, evita sanciones derivadas de la responsabilidad empresarial, mayor resultado operacional, entre otros.

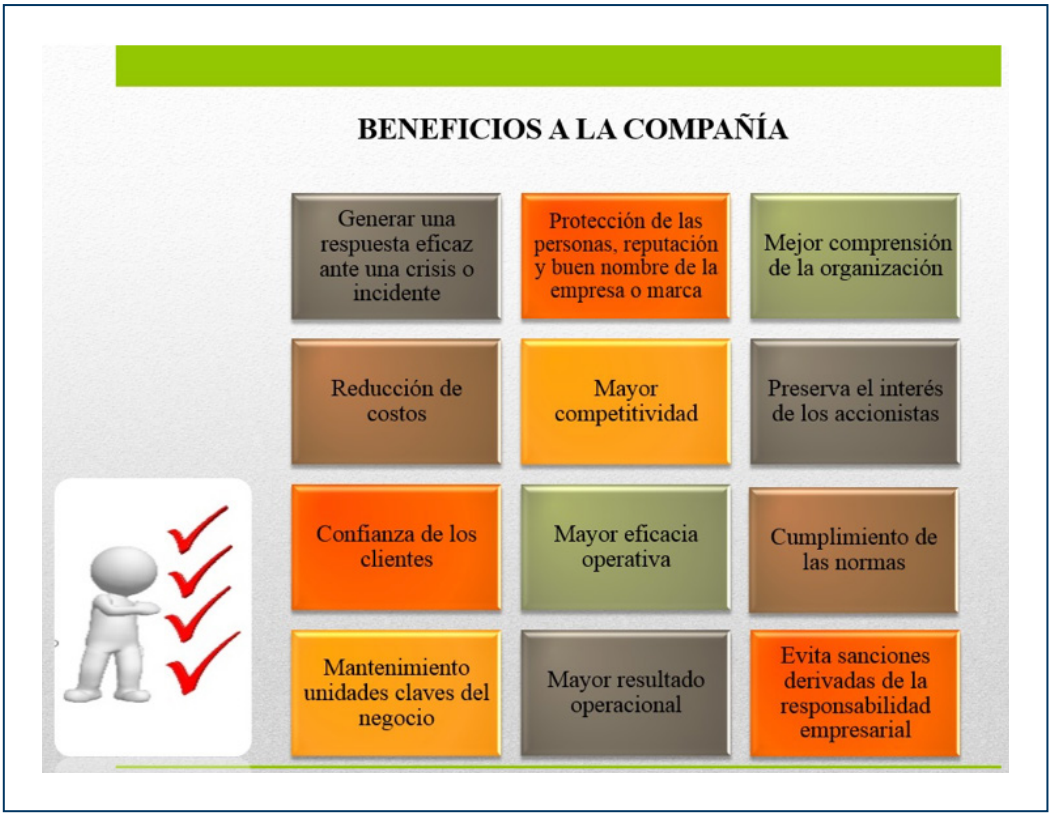


Figura 1
Fuente: propia

En La estructura de la norma ISO 22301 existen una serie de cláusulas entre las cuales se destacan:

- Clausula 4: Contexto de la organización
- Clausula 5: Liderazgo
- Clausula 6: Planificación
- Clausula 7: Apoyo
- Clausula 8: Operación
- Clausula 9: Evaluación de desempeño
- Clausula 10: Mejoramiento

Gestión de la Continuidad del Negocio

Plan de continuidad del negocio

Plan desarrollado por la empresa ante situaciones de riesgo, necesario en toda empresa sin importar su fin, tamaño u objetivo, ni el costo que este implique. Este plan debe apuntar a minimizar el riesgo de interrupción de actividad de la empresa y de presentarse la interrupción garantizar que el tiempo de dicha interrupción sea el mínimo posible, manteniendo el nivel de servicio establecido por la compañía.

El restablecimiento del servicio y/o proceso afectado debe darse de acuerdo a la criticidad del mismo, de presentarse varios incidentes simultáneos y no poder solucionarlos al mismo tiempo se debe comenzar por el más crítico o necesario para dar continuidad al negocio.

Figura 2
Fuente: propia

Una vez sorteada la incidencia se debe proceder a analizar y documentar las acciones desarrolladas y los resultados obtenidos, así mismo analizar los motivos de la falla para generar actividades tendientes a la no repetición, aprendiendo de lo sucedido y mejorando el tiempo de respuesta ante dicha incidencia.

Elementos del plan de continuidad del negocio

Figura 3
Fuente: propia

1. Análisis de posibles situaciones: definición y análisis de posibles situaciones e incidencias que se podrían presentar, estas deben contar con:
   - Que o quien podría provocar la incidencia.
   - Que daño puede causar.
   - Quien es el primer respondiente a esta incidencia.
   - Acciones a tomar una vez generada la incidencia y pasos a seguir ante el incidente.
   - Documentar y registrar la incidencia para su posterior análisis y acciones de mejora.
2. Definición de Situaciones Críticas: en este apartado se analizarán los eventos e incidencias que NO se pueden evitar través de las medidas implementadas.
3. Comité de emergencia: personal capacitado en manejo de crisis y serán los encargados de gestionar la situación ante una incidencia.

Los planes de continuidad del negocio deben ser probados y mejorados antes de aplicarlos, al igual que divulgados a todo el personal implicado en la situación, de lo contrario se podría empeorar dicha situación.

Figura 5
Fuente: propia

Fases para el desarrollo del plan de continuidad del negocio (ISO 22301)

1. Definición del proyecto: en esta fase se establecerán los objetivos, el alcance y los diversos escenarios.
2. Análisis del impacto (BIA Business Impact Analysis): en esta fase se realiza el análisis de riesgos, el impacto del incidente, tiempos de recuperación, coberturas de seguros.
3. Selección de estrategias: definir con qué recursos se cuenta, establecer las estrategias de recuperación que más le convenga a la empresa (interna o externa) analizar ventajas y desventajas de cada una de ellas.
4. Desarrollo de planes: implementación de procesos y procedimientos para afrontar las incidencias.
5. Pruebas y mantenimiento: desarrollo de pruebas periódicas del plan de continuidad para encontrar y corregir falencias, se deben incluir actualizaciones del sistema, verificación de copias de seguridad, coordinación del personal, verificación de conectividad y rendimiento de los sistemas, verificación de procedimientos para la notificación de incidencias.

Relación con otras Normas

La norma ISO 22301 está estrechamente relacionada a la Norma ISO 27001 SGSI sistema de gestión de seguridad de la información la cual exige en su capítulo 1, anexo A de los controles el 14 Continuidad del negocio, es decir si se quiere orientar, alinear, certificar seguridad de la información me dice que desarrolle planes para la continuidad del negocio para lo cual me indica que debo tener y presenta una guía de cómo realizarlo.

Relación con BS2599 norma británica antecesora de la ISO 22301 por lo cual es importante trabajar de la mano de dicha norma.

También se relaciona con la Norma ISO 9000 Sistema de gestión de la calidad y la ISO 14000 Sistema de gestión ambiental SGA.

En la siguiente imagen se resume la gestión de continuidad del negocio:

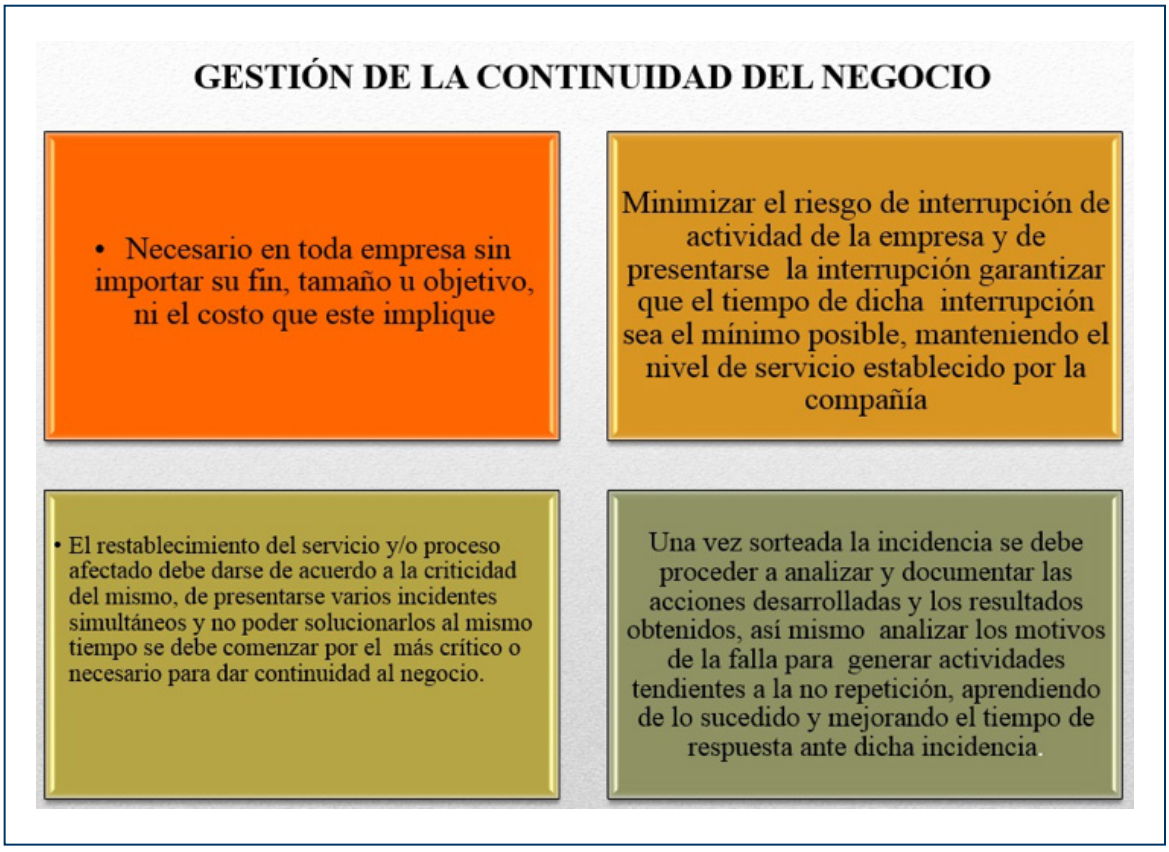


Figura 4
Fuente: propia

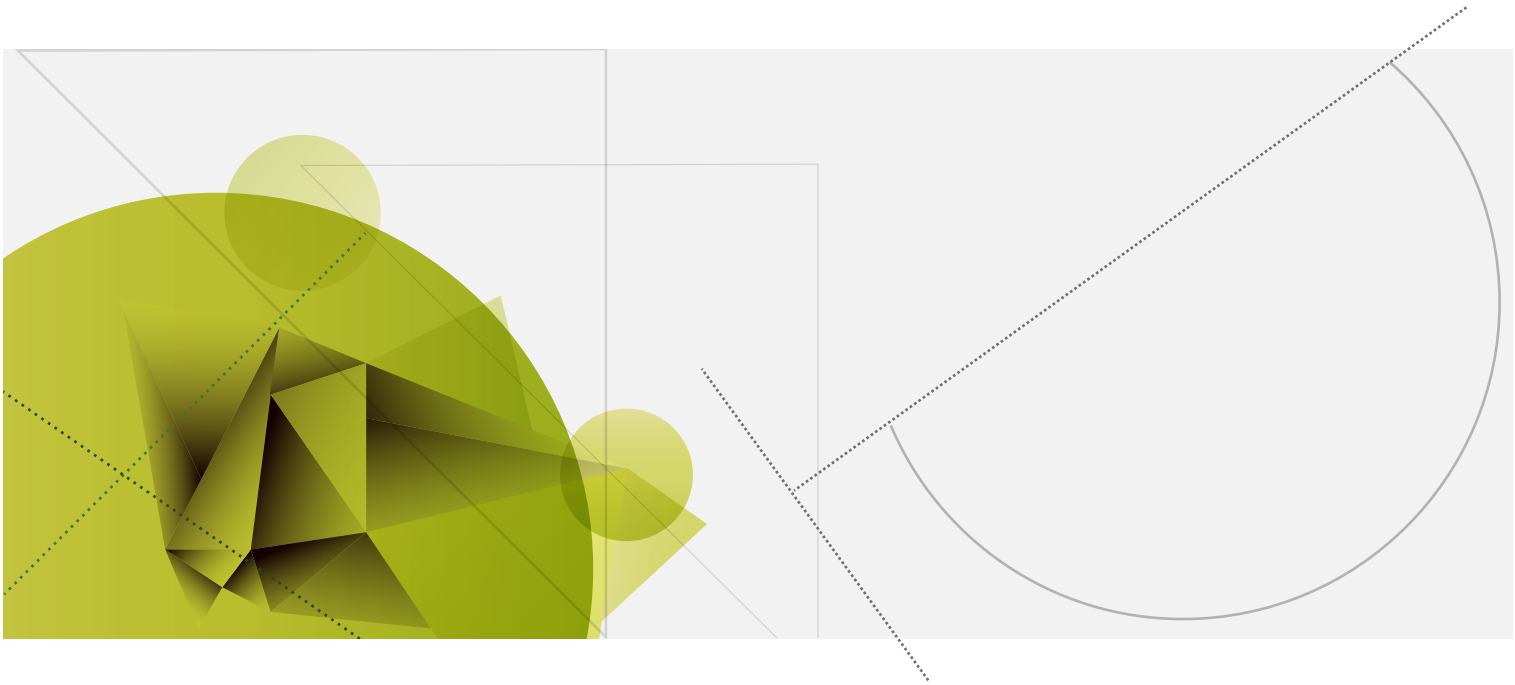
Remisión a fuentes complementarias

Lo invitamos a visitar la página del ministerio de TIC www.mintic.gov.co donde encontrara la Guía 10, Guía para la preparación de las TIC para la continuidad del negocio, Seguridad y Privacidad de la Información.

Bibliografia

- Comisión Interamericana de Telecomunicaciones. (2009). Guía de gestión de riesgos para sistemas de tecnologías de la información.
- CONPES 3701. (2011). Lineamientos de Políticas Para la Ciberseguridad y Ciberdefensa en Colombia.
- ISO/IEC. (s.f.). Guía 73 Gestión de riesgos, directrices de uso y normas.
- ISO/IEC 13335-1. (2004). Gestión de la Seguridad de las Tecnologías de la Información y la comunicación.
- ISO/IEC 13335-4. (2000). Directrices para la gestión de la seguridad.
- ISO/IEC 17799. (2005). Técnicas de seguridad- Código para la práctica de la gestión de seguridad de la información.
- ISO/IEC 22301. (2012). Sistema de Gestión de Continuidad del Negocio.
- ISO/IEC 27001. (2005) SGSI: Sistemas de Gestión de la Seguridad de la Información, Asociación española de Normalización y Certificación.
- ISO/IEC TR 18044. (2004). Gestión de Incidencias de Seguridad de la Información.
- OCDE. (2016). Directrices para la seguridad de los sistemas y redes de información. Hacia una cultura de la seguridad. Paris: OCDE.
- MINTIC. (2016). Gestión de incidentes de Seguridad.
- Reina, E., y Morales, J. (2014). Análisis de Normas Internacionales ISO/IEC 27000 para Gestionar el riesgo de Seguridad de la Información. Universidad Tecnológica de Pereira.
- TechNet. (2016). Respuesta a incidentes de Seguridad, Microsoft.

Esta obra se terminó de editar en el mes de noviembre
Tipografá Myriad Pro 12 puntos
Bogotá D.C,-Colombia.



AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO