DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN QUE PERMITA APOYAR A LA SUBGERENCIA DE INFORMÁTICA Y TECNOLOGÍA DE LA EMPRESA DE TELECOMUNICACIONES DE BUCARAMANGA TELEBUCARAMANGA S.A – E.S.P EN EL PROCESO DE CERTIFICACIÓN EN ISO 27000.

HARRISON TAMIR VELASCO H. ID: 69728

UNIVERSIDAD PONTIFICIA BOLIVARIANA
ESCUELA DE INGENIERÍAS Y ADMINISTRACIÓN
FACULTAD DE INGENIERÍA INFORMÁTICA
FLORIDABLANCA
2008

DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN QUE PERMITA APOYAR A LA SUBGERENCIA DE INFORMÁTICA Y TECNOLOGÍA DE LA EMPRESA DE TELECOMUNICACIONES DE BUCARAMANGA TELEBUCARAMANGA S.A – E.S.P EN EL PROCESO DE CERTIFICACIÓN EN ISO 27000.

HARRISON TAMIR VELASCO H. ID: 69728

Informe final de la práctica empresarial desarrollada como requisito para optar al titulo de INGENIERO INFORMÁTICO

Supervisor: Ing. WILSON CASTAÑO GALVIZ MSc

UNIVERSIDAD PONTIFICIA BOLIVARIANA
ESCUELA DE INGENIERÍAS Y ADMINISTRACIÓN
FACULTAD DE INGENIERÍA INFORMÁTICA
FLORIDABLANCA
2008

NOTA DE ACEPTACION

_____

_____

_____

Calificador1

_____

Calificador2

_____

Calificador3

_____

BUCARAMANGA DIA: ____ MES: ____ AÑO: 2008

DEDICATORIA

Ofrezco este triunfo a mi Dios y Salvador por permitirme culminar una etapa más mi camino.

A mis padres, TAMIR VELASCO FLOREZ y ELSA HERRERA, que me dieron la vida, el amor incondicional y la formación necesaria para poder realizar mis metas.

A mis hermanos Sandra Milena, Mónica Liliana, Iván Dario y familia en general, que mediante su constante preocupación y apoyo, me demostraron que cuento con un gran respaldo que me fortalece.

Harrison Tamir Velasco H.

.

AGRADECIMIENTOS

A mis padres y hermanos por su paciencia, comprensión, compromiso y ánimo permanente.

A la universidad representada en los trabajadores de cada dependencia y sus docentes, por brindarme la oportunidad de adquirir conocimientos y experiencias que contribuyeron a mi crecimiento como persona y como profesional.

A WILSON, ELKIN y ANGELICA, mis profesores de toda la carrera, por su ética, dedicación, compromiso y responsabilidad.

A Diego P, Diego R, Julián, Mateo, Andrés f, Maria José y July, compañeros de estudio y grandes amigos que permanecieron conmigo en las buenas y en las malas y me animaron a continuar adelante.

A Alejandra que me acompañó y me ofreció su amor incondicional.

A todos y cada una de las personas que contribuyeron a que esta meta llegara a su final.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

RESUMEN GENERAL DE TRABAJO DE GRADO

TITULO: DISEÑAR EL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN QUE PERMITA APOYAR A LA SUBGERENCIA DE INFORMÁTICA Y TECNOLOGÍA DE LA EMPRESA DE TELECOMUNICACIONES DE BUCARAMANGA TELEBUCARAMANGA S.A – E.S.P EN EL PROCESO DE CERTIFICACIÓN EN ISO 27000.

AUTOR: Harrison Tamir Velasco Herrera.

FACULTAD: Facultad de Ingeniería Informática

DIRECTOR(A): Wilson Castaño Galviz

RESUMEN

La Subgerencia de Informática y Tecnología de Telebucaramanga S.A – E.S.P es conciente de la evolución de las normas que se especializan en la gestión y seguridad de la información, por esta razón quiere asumir el reto y busca administrar de una forma adecuada la seguridad de la infraestructura tecnológica a cargo de esta dependencia, para ello requiere diseñar el sistema de gestión de la seguridad de la información con base en la norma ISO 27000 y en este proceso evaluar una posible certificación en la norma, garantizado de esta manera la continuidad del negocio y confiabilidad en la toma de decisiones. Empresas como Asociación Latinoamericana de Profesionales de Seguridad Informática de Colombia, ATH y Bancafé entre otras han implementado la norma, gestionando de forma segura y confiable la información. Este documento establece un diseño preliminar que permite apoyar a la Subgerencia en este proceso de certificación, involucrando plan estratégico de la organización, el recurso humano y todos los entes que interactúan con las TI , definiendo los controles mas relevantes de la norma que se ajustan a la empresa, políticas de seguridad, vulnerabilidades, amenazas y riesgos de la información, dejando al descubierto que la subgerencia puede gestionar la documentación pertinente para lograr la certificación, sin dejar a un lado fallas por falta de recurso humano calificado, ejemplo de ello es que la administración de la red, base de datos y la seguridad de la información son manejadas por una sola persona y que algunos servidores que prestan servicio corporativo no cuentan con un respaldo hardware para suplir algún tipo de eventualidad.

PALABRAS CLAVE:
Tecnologías de Información, Gobierno Corporativo, Riesgo, Vulnerabilidad, Amenazas y Seguridad.

GENERAL SUMMARY OF WORK OF DEGREE

TITLE: DESIGN THE MANAGEMENT SYSTEM OF INFORMATION SECURITY THAT ALLOWS TO SUPPORT THE ASSISTANT MANAGER OF INFORMATICS AND TECHNOLOGY OF EMPRESA DE TELECOMUNICACIONES DE BUCARAMANGA TELEBUCARAMANGA SA – ESP IN THE CERTIFICATION PROCESS OF ISO 27000.

AUTHOR: Harrison Tamir Velasco Herrera.

ACADEMIC PROGRAM: Facultad de Ingeniería Informática

MANAGER: Wilson Castaño Galviz

ABSTRACT

The Assistant Manager of Informatics and Technology of Telebucaramanga SA - ESP is aware of the evolution of standards that specialize in management and information security, for this reason wants to take the challenge and find an appropriate way to manage security technological infrastructure in charge of this unit, for this purpose, it requires to design the management system of information security based on ISO 27000 and in this process to evaluate a possible standard certification, thus ensuring business continuity and reliability in decision making. Companies such as Asociación Latinoamericana de Profesionales de Seguridad Informática de Colombia, ATH and Bancafé among others have implemented the norm, managing secure and reliable information. This document provides a preliminary design that allows support to the Assistant Manager in this certification process, involving the organization's strategic plan, human resources and all entities that interact with IT, defining the most important controls of the standard that fit the company, security policies, vulnerabilities, threats and risks to information, revealing that the assistant manager can manage all relevant documentation to achieve certification, and with faults aside for lack of qualified human resources, example of this is that the network administration, database and information security are handled by one person and that some serving corporate servers do not have a hardware to support any eventuality.

KEYWORDS:
Information Technology, Corporate Governance, Risk, Vulnerability, Threats and Security.

1. INTRODUCCION

Manejar la información de una forma dinámica, clara y sin alteraciones es de vital importancia en el proceso de toma de decisiones ante cualquier negocio, las tecnologías de información han evolucionado en su proceso de diseño, implementación y control, incluyendo en estas etapas la estructura organizacional, las estrategias del negocio, el recurso humano y todas las entidades que directa o indirectamente alteran el comportamiento de la compañía, este tipo de planteamiento permite que las dependencias de la organización manejen los mismos objetivos, estrategias y parámetros, por esta razón la información que la compañía maneja debe ser confiable y segura para evitar alteraciones en la toma de decisiones de la compañía.

Las organizaciones comprenden hoy día que es necesario invertir en infraestructura tecnológica, pero paralelamente a esto el crecimiento de dicha tecnología aumenta el grado del riesgo y a su vez la intensificación de los controles y políticas de seguridad. Si por algún motivo estas inversiones son sujetas a delitos informáticos, errores humanos, fallas en el sistema las perdidas en el negocio pueden llegar a ser significativas y en su defecto pueden llegar a superar el monto de la inversión. Es de suma importancia destacar que las TI no se limitan a los profesionales en informática si no que están diseñadas para casi todo tipo de población que quiera explorar en estos temas, además las organizaciones exigen y capacitan a el personal en sus sistemas de información y en algunos casos en su infraestructura tecnológica aumentando los riesgos que pueden sufrir las TI.

Los delitos informáticos perjudican a cualquier empresa alterando la estabilidad del negocio, partiendo de esto se hace necesario definir el sistema de gestión de

la seguridad de la información (SGSI)[1], permitiendo planear, implementar, monitorear y controlar la seguridad de la información. Muchas empresas Colombianas han asumido este reto participando en la elaboración, estructuración y certificación de la norma ISO 27000[2] (Seguridad de la información) mientras que otras empresas la están aplicando para su mejoramiento.

Este documento pretende destacar la importancia de tener definida una administración adecuada para disminuir considerablemente el riesgo, gestionando políticas de seguridad informática, herramientas y metodologías que permitan diagnosticar de manera pertinente cualquier tipo de eventualidad que pueda perjudicar la estabilidad del negocio.

[1] ICONTEC, COMPENDIO Sistema de Gestión de la Seguridad de la Información. (SGSI). Colombia: ICONTEC 2006. p. 20-21.
[2] Ibid. p. 12-13.

2. OBJETIVOS

2.1 OBJETIVOS GENERAL

- Diseñar el Sistema de Gestión de la Seguridad de la Información que permita apoyar a la Subgerencia de Informática y Tecnología de la Empresa de Telecomunicaciones de Bucaramanga TELEBUCARAMANGA S.A – E.S.P en el proceso de certificación en ISO 27000.

2.2 OBJETIVOS ESPECÍFICOS

- Revisar el estado del arte de la Seguridad de la Información teniendo en cuenta la normatividades que se aplican en este campo.
- Determinar el estado actual del manejo de la Seguridad de la Información en la Subgerencia de Informática y Tecnología teniendo como parámetro de referencia la Norma ISO-27000.
- Establecer el Mapa de Riesgos Tecnológicos y de Información al interior de la Subgerencia de Informática y Tecnología para determinar posibles vulnerabilidades de alteración de la información.
- Documentar las Políticas de Seguridad de la Información aplicable para la Empresa de Telecomunicaciones de Bucaramanga – TELEBUCARAMANGA S.A – E.S.P en el departamento de Informática y Tecnología.

- Definir los controles aplicables de la norma ISO 27000 para el seguimiento del desempeño y la efectividad del Sistema de Gestión de la Seguridad de la Información.
- Instalar y configurar Software corporativo de usuario final en los equipos de los funcionarios de TELEBUCARAMANGA y sus respectivas sucursales en la ciudad de Bucaramanga.

3. GENERALIDADES DE LA EMPRESA

3.1 Nombre de la empresa

TELEBUCARAMANGA S.A –E.S.P

3.2 Descripción de la empresa

Telebucaramanga es una compañía que brinda servicios de telecomunicaciones en Colombia específicamente en Santander, proporcionando soluciones que se ajusten a las condiciones socioeconómicas y culturales de sus clientes. Actualmente la compañía TELEFÓNICA de España adquirió el 51 % de acciones de Telebucaramanga convirtiéndose en el mayor accionista de la compañía, por esta razón es una empresa que promete con esta negociación evolucionar frente a las exigencias tecnológicas y comerciales del mercado mundial.

3.3 Servicios

1. Los servicios básicos de la Compañía incluyen: (a) Telefonía local, local extendida y social; (b) larga distancia nacional e internacional a través de la Empresa Nacional de Telecomunicaciones ("Telecom"), Orbitel y la Empresa de Telecomunicaciones de Bogotá ("ETB"); (c) telefonía celular, con base en los contratos suscritos con los distintos operadores del servicio a nivel nacional, y (d) Internet y transmisión de datos punto a punto entre

otros. La compañía puede prestar los servicios portadores en el ámbito de su jurisdicción y adicionalmente, cuenta con la prestación de servicios especiales como transferencia de llamadas, código secreto, despertador automático, marcación abreviada, conferencia, llamada en espera, no molestar, usuario ausente, y marcación directa a extensiones. TELEBUCARAMANGA también ha introducido nuevos servicios de valor agregado; e) Televisión satelital a través de la compañía Telefónica.[3]

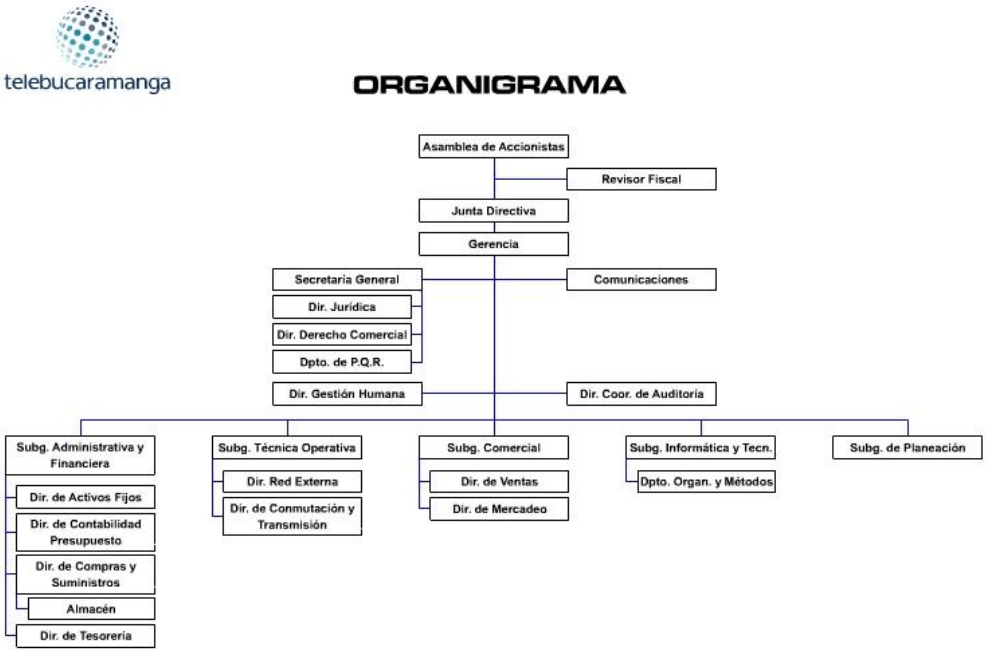
3.4 Numero de empleados

1. 267 de planta

250 indirectos (practicantes, contratistas, etc.)

3.5 Estructura organizacional[4]

Figura 1: Organigrama.



[3] Información Disponible en: http://www.telebucaramanga.com.co/code/index_telebu.jsp

[4] Figura 1. Tomada de: Archivos de la subgerencia de informática y tecnología de TELEBUCARAMANGA S.A –E.S.P

Teléfono:

6309600 - 6336282 – 113

Dirección:

Carrera 36 con calle 15 Esquina

3.6 Reseña histórica

En 1886, llegaron a Bucaramanga los primeros aparatos telefónicos traídos por los alemanes Cristian P. Clausen y Koppel, quienes en medio de la admiración de los lugareños exhibieron y probaron estos aparatos en sus almacenes. El 20 de junio de 1888 se constituyó una sociedad, conformada por los señores Eliseo Camacho (quien había obtenido del Concejo Municipal la concesión de operar esta tecnología en la ciudad por treinta años), Cayetano González, Hermógenes Motta y José Antonio Serrano; la llamada inaugural se realizó el día 1 de noviembre de 1888 y en poco tiempo la localidad contaba con 35 suscriptores, los cuales eran en su mayoría extranjeros. De esta manera Bucaramanga, para esa época se convertía en la tercera ciudad en Colombia en tener una empresa de teléfonos, la cual dos años más tarde vería extendida su cobertura a Piedecuesta, Floridablanca y Puerto Botijas sobre el río Lebrija, este servicio era prestado con equipos de magneto (tecnología de punta en Colombia).

La sociedad, bajo la dirección del señor Eliseo Camacho, cumplió su plan estratégico durante los primeros años de labores, atendiendo las llamadas locales y de larga distancia con poblaciones vecinas, hasta que el Ejercito Conservador la tomó en medio de la guerra civil; más tarde, el jefe civil y militar del departamento de Santander el general Ramón González Valencia en 1903 la entregó al departamento y éste en 1912 cedió los equipos al municipio.

Hacia 1916 la antigua empresa de Teléfonos de la Provincia de Soto se transformó en la Empresa de Teléfonos de Santander, sociedad anónima de carácter privado que llevó el servicio telefónico a gran parte del departamento de Santander, ya a partir del año 1955 se comenzó a prestar el nuevo servicio automático de líneas directas, con discado, que permitía en ese entonces la comunicación sin intermedio de una operadora.

En 1962 la empresa fue vendida al municipio, que entró a realizar una reingeniería al interior de la compañía, quedando como administradora de los teléfonos la GENERAL TELEPHONE Co, entidad financiadora, una vez que la Empresa Telefónica de Santander S.A. vendiera el resto de sus líneas al departamento y se liquidara en 1.962 el Municipio de Bucaramanga compra La Empresa Telefónica de Santander (Empresa Privada) la central y las redes urbanas que dicha empresa tenía en Bucaramanga.

La Empresa de Telecomunicaciones de Bucaramanga S.A. E.S.P - TELEBUCARAMANGA - inicia labores como establecimiento público en 1972 bajo la denominación de Empresas Públicas de Bucaramanga, con el fin de prestar los servicios públicos en los municipios de Bucaramanga, Girón y Floridablanca en el Departamento de Santander.

Desde su comienzo la empresa fue controlada por el Municipio como entidad descentralizada, prestando los servicios de Telefonía Básica Conmutada, Aseo, Plazas de mercado y matadero, además de contar con otras inversiones.

Mediante la escritura pública No. 1435, registrada el 23 de mayo de 1997 en la Notaría 06 del Círculo de Bucaramanga, inscrita en Cámara de Comercio el 30 de mayo de 1997 y por medio del acuerdo 014 del Consejo Municipal se ordenó la transformación de Empresas Públicas de Bucaramanga en una sociedad de economía mixta, bajo los términos de la Ley 142 de 1.994, para lo cual se constituyó la sociedad denominada Empresas Públicas de Bucaramanga E.S.P conforme a las disposiciones de la Ley 142 de 1994. De acuerdo con la escritura

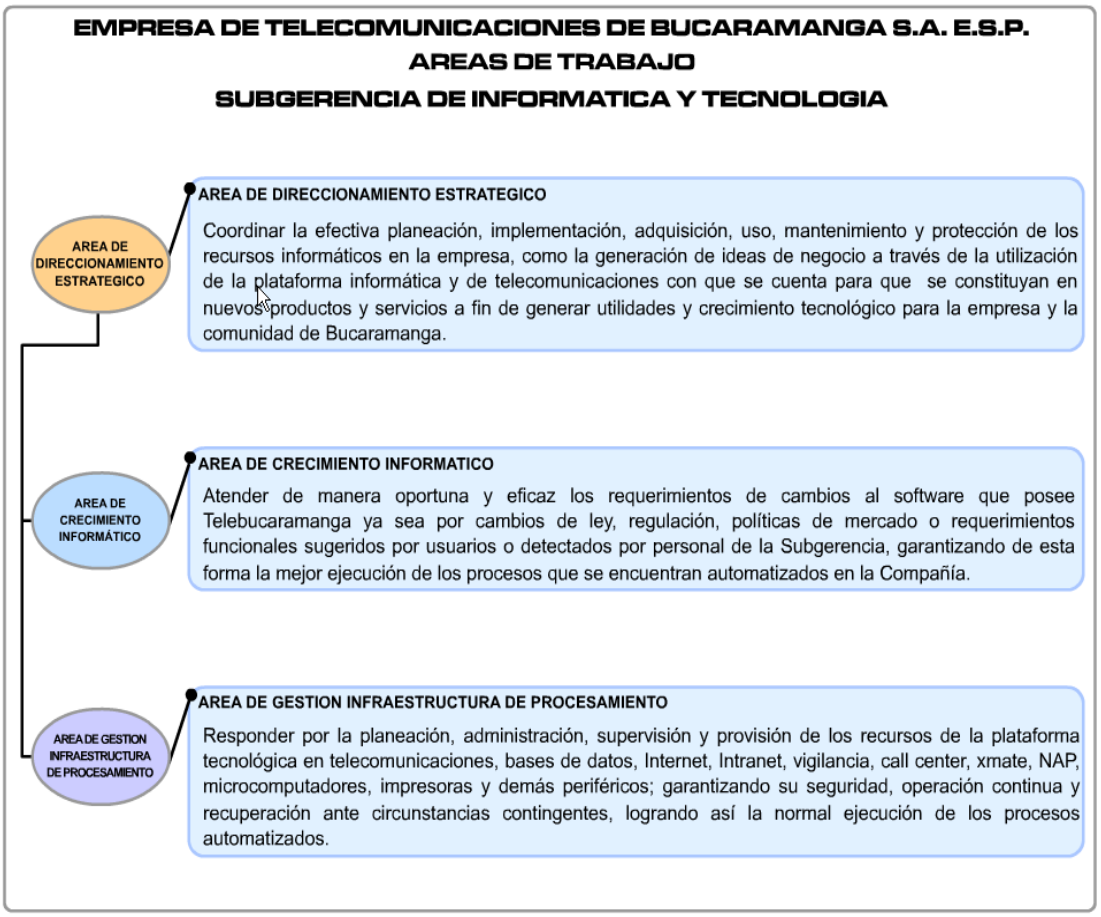
pública No. 3408 del 8 de octubre de 1998 se llevó a cabo el proceso de escisión parcial mediante el cual Empresas Públicas de Bucaramanga E.S.P actúa como escidente, creándose dos sociedades de economía mixta: Empresas de Aseo de Bucaramanga S.A. E.S.P y Sociedad de Inversiones Bucaramanga S.A. como sociedades beneficiarias. Este proceso finalizó el 30 de octubre de 1998. En la escritura pública No. 720 del 17 de marzo de 1999 otorgada en la Notaría 01 de Bucaramanga, inscrita en Cámara de Comercio el 19 de marzo de 1999 consta el cambio de razón social a Empresas Públicas de Bucaramanga S.A. E.S.P. Después de la escisión, la empresa vendió el 55.999994% de su capital a la Empresa Nacional de Telecomunicaciones-TELECOM-. Cambiando así su razón social, según escritura pública No. 925 del 26 de abril de 2.000, corrida en la notaría Primera del Círculo de Bucaramanga e inscrita en Cámara de Comercio el 01 de Agosto de 2002, se da el cambio de denominación social a Empresa de Telecomunicaciones de Bucaramanga S.A. E.S.P Telebucaramanga, empresa con autonomía administrativa, patrimonial y presupuestal, que ejerce sus actividades dentro del ámbito del derecho privado.

Hoy en día, TELEBUCARAMANGA es el cuarto operador del servicio de Telefonía Pública Básica Conmutada ("TPBC") en Colombia y atiende una población estimada de 847.175 habitantes. A diciembre de 2000, la Compañía contaba con 274.986 líneas en planta interna y 222.896 líneas en servicio, lo que representaba una densidad de 25.64% en el mercado.[5]

[5] Nuestra Compañía. Reseña histórica Disponible en: http://www.telebucaramanga.com.co/code/index_telebu.jsp

3.7 Descripción Del Área de Práctica[6]

Figura 2: Áreas de trabajo Subgerencia de Informática y Tecnología.



Nombre del director:

Javier Enrique Mariño.

[6] Figura 2. Tomada de: Archivos de la subgerencia de informática y tecnología de TELEBUCARAMANGA S.A –E.S.P

4. PLAN DE TRABAJO PROPUESTO

4.1 OBJETIVOS ESPECÍFICOS

- Revisar el estado del arte de la Seguridad de la Información teniendo en cuenta la normatividades que se aplican en este campo.
- Determinar el estado actual del manejo de la Seguridad de la Información en la Subgerencia de Informática y Tecnología teniendo como parámetro de referencia la Norma ISO-27000.
- Establecer el Mapa de Riesgos Tecnológicos y de Información al interior de la Subgerencia de Informática y Tecnología para determinar posibles vulnerabilidades de alteración de la información.
- Documentar las Políticas de Seguridad de la Información aplicable para la Empresa de Telecomunicaciones de Bucaramanga – TELEBUCARAMANGA S.A – E.S.P en el departamento de Informática y Tecnología.
- Definir los controles aplicables de la norma ISO 27000 para el seguimiento del desempeño y la efectividad del Sistema de Gestión de la Seguridad de la Información.
- Instalar y configurar Software corporativo de usuario final en los equipos de los funcionarios de TELEBUCARAMANGA y sus respectivas sucursales en la ciudad de Bucaramanga.

4.2 ACTIVIDADES

- Elaborar un informe del estado actual de la Seguridad de la Información en TELEBUCARAMANGA S.A- E.S.P de acuerdo con la norma ISO 27000.
- Identificar las amenazas y vulnerabilidades en el manejo de la Información, estableciendo niveles de impacto para cada una de ellas.
- Determinar la matriz de riegos de los activos que conforman la plataforma tecnológica y de información de TELEBUCARAMANGA S.A – E.S.P.
- Elaborar un documento que contenga un Análisis y evaluación de los riesgos de la información en el departamento de Informática y Tecnología que permita identificar acciones, recursos, responsabilidades y prioridades en TELEBUCARAMANGA S.A –E.S.P.
- Documento final con Diseño del Sistema de Gestión de la Seguridad de la Información propuesto para TELEBUCARAMANGA S.A – E.S.P.
- Instalar y configurar Software corporativo de usuario final en los equipos de los funcionarios dentro de las instalaciones TELEBUCARAMANGA y sus respectivas sucursales en la ciudad de Bucaramanga.
- Prestar el soporte técnico a funcionarios de Telebucaramanga en problemas presentados en el Software Corporativo a nivel de usuario final cuando se presente una sobrecarga en el trabajo del equipo de soporte.

5. MARCO TEÓRICO

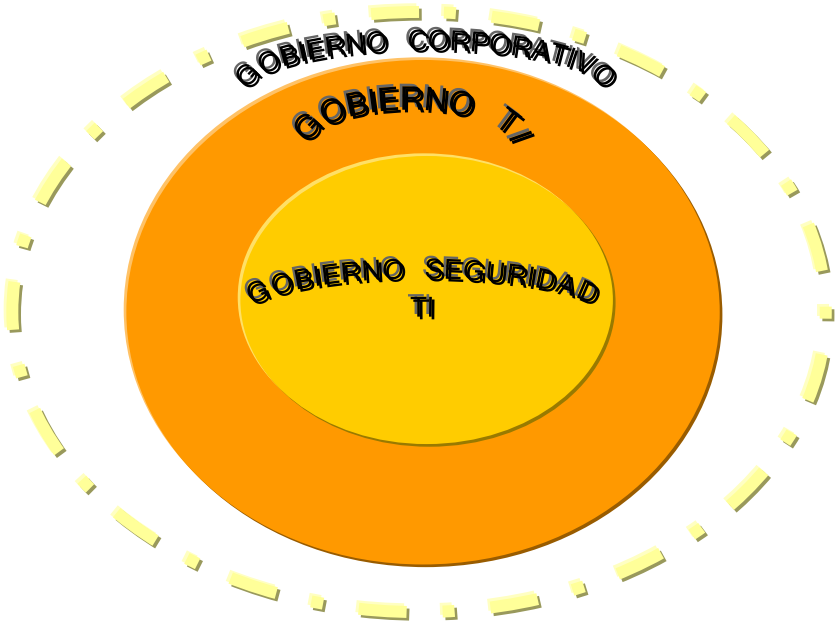
El manejo de la información en cualquier tipo de organizaciones es fundamental en los procesos de toma de decisiones y direccionamiento del negocio, teniendo en cuenta la planeación, las estrategias, el control y la estructura organizacional, pero en muchas de estas empresas cada dependencia que conforma la estructura de la organización posee sus propios objetivos, prioridades y arrojan sus propios resultados (ver figura 3), además la información que comparten entre ellas en algunas ocasiones presentan conflictos de comunicación, sin darse cuenta que tienen un mismo objetivo corporativo en común, sumado a esto los resultados que visionan los entes administradores (gerencia) no son tomados en cuenta en la elaboración de objetivos por dependencia.

Figura 3: CONFLICTO DE COMUNICACIÓN ENTRE DEPENDENCIAS

Fuente: Adaptado de http://www.ieee.org.ar/downloads/2006-hrabinsky-itil.pdf

La evolución en las tecnologías informáticas hace necesario una reestructuración en la forma como se planea e implementa nueva tecnología en las organizaciones, estas exigen un estudio previo de la empresa en todas sus estructuras, objetivos y procesos, para lograr un óptimo desempeño en la aplicación de los SI, por esta razón se ha venido involucrando un nuevo concepto que se denomina gobierno de TI. (Ver figura 4).

Figura 4: El Gobierno de TI como parte de un marco de Gobierno Corporativo



Fuente: Adaptado de: http://www.acis.org.co/fileadmin/Base_de_Conocimiento/XXVI_Salon_Informatica/RobertoArbelaezXXVISalon2006.pdf

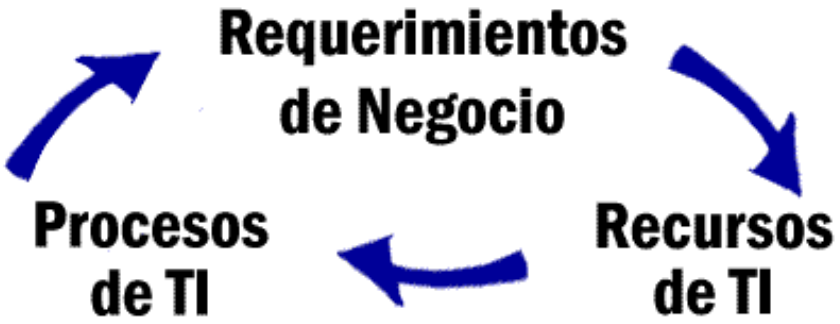
De esta manera las normas orientadas al manejo de la información han evolucionado, analizan como esta constituido el gobierno corporativo de la organización, como se encuentra estructurado, quien lo conforma, que niveles existen, que procesos y procedimientos llevan acabo, teniendo como prioridad el direccionamiento, visión, misión, mercado, estrategias de negocio, que pretenden alcanzar y de esta forma poder definir los lineamientos, características, objetivos y adquisición de nuevas tecnologías de información para suplir la verdadera

necesidad de la organización, optimizando recursos hardware, software y disminuyendo el riesgo en la seguridad de la forma mas adecuada.

5.1 COBIT

(Gobernabilidad, Control y Auditoria de Información y Tecnologías Relacionadas)[7] es un gran exponente de esta evolución, ya que los lideres, las estructuras y los procesos organizacionales conforman la herramienta de gobierno de TI que ayuda a comprender y administrar los riesgos asociados con tecnología de información y con tecnologías relacionadas. El concepto se aplica a todos los sistemas de información que maneje la organización, logrando que los procesos manejen información pertinente y confiable. Para que esto funcione es necesario tener claro el significado y la forma como interactúan 3 pilares fundamentales que plantea COBIT. (Ver Fig. 5)

Figura 5: Pilares fundamentales de COBIT



Fuente: http://200.5.106.140/academicas/catedras/Seguridad%20y%20Control%20Informatico/AS_COBIT.ppt.

[7] ELISSONDO, Luis. Auditoría y Seguridad de Sistemas de Información. http://200.5.106.140/academicas/catedras/Seguridad%20y%20Control%20Informatico/AS_COBIT.ppt

5.1.1 Requerimientos de negocio.[8]

- **Calidad**: Atributos, costo, entrega de producto o servicio que se ofrece en el negocio.
- **Fiduciarios:** Cumplimiento de todas normas nacionales y en su defecto internacionales que rigen los sistemas informáticos según las características negocio.
- **Seguridad:** Todo sistema SI debe manejar unas cualidades mínimas de toda la información que este inmersa en el, definiendo en su defecto las restricciones de información del negocio.

Figura 6: Cualidades de la información.

Efectividad	Se refiere a que la información relevante sea pertinente para el proceso del negocio, así como a que su entrega sea oportuna, correcta, consistente y de manera utilizable.
Eficiencia	Se refiere a la provisión de información a través de la utilización óptima (más productiva y económica) de recursos.
Confidencialidad	Se refiere a la protección de información sensible contra divulgación no autorizada.
Integridad	Se refiere a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.
Disponibilidad	Se refiere a la disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.
Cumplimiento	Se refiere al cumplimiento de aquellas leyes, regulaciones y acuerdos contractuales a los que el proceso de negocios está sujeto, por ejemplo, criterios de negocio impuestos externamente.
Confiabilidad de la información	Se refiere a la provisión de información apropiada para la administración con el fin de operar la entidad y para ejercer sus responsabilidades de reportes financieros y de cumplimiento.

Fuente: http://200.5.106.140/academicas/catedras/Seguridad%20y%20Control%20Informatico/AS_COBIT.ppt

[8] ELISSONDO, Op. cit., Auditoria y Seguridad de Sistemas de Información.

5.1.2 Recursos de TI.[9]

- **Datos:** Cualquier tipo de elemento externo o interno que interfiera y/o altere el sistema de información.
- **Aplicaciones**: Es un manejo manual y programado de procedimientos dando como resultado un sistema de aplicación.
- **Tecnología:** Es todo lo relacionado con el software y hardware que posee el sistema de información. (Sistemas operativos, servidores, redes, etc.).
- **Instalaciones:** La ubicación física donde se mantienen en un estado optimo los sistemas de información y poder dar soporte a estos.
- **Personal:** El recurso humano que interactúa con los sistemas de información del negocio.

5.1.3 Procesos de TI.[10]

- **Planeación y organización:** La forma como se va a llevar acabo el direccionamiento, la ejecución y las estrategias de negocio. Estas deben ser planeadas, comunicadas, administradas y lo mas importante controladas para definir que tipo de tecnología de la información es la apropiada, teniendo presente todo lo que en el plan se concluyo.
- **Adquisición e implementación:** Estas herramientas lógicas y físicas deben adaptarse estratégicamente dando una o más soluciones a la organización y esa fusión debe ser orientada al concepto de las TI.
- **Soporte:** Las TI están sujetas a ser alteradas por diferentes circunstancias que en algún momento pueden llegar a entorpecer el buen funcionamiento del sistema de información, por esta razón se hace necesario realizar

[9] ELISSONDO, Op. cit., Auditoria y Seguridad de Sistemas de Información.
[10] Ibid. Auditoria y Seguridad de Sistemas de Información.

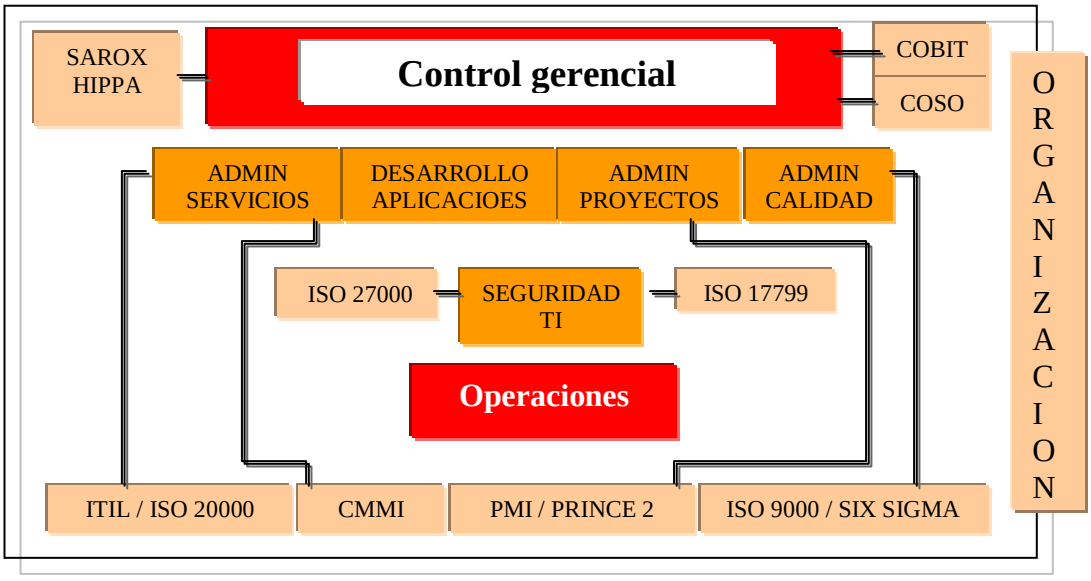
mantenimientos correctivos que solucionen cualquier tipo de alteración ocurrida en cualquier punto de las TI.

- **Monitoreo:** Todos los procesos que están inmersos en las TI están sujetos a ser evaluados regularmente de una forma preventiva verificando su calidad y suficiencia de acuerdo a los requerimientos de control previamente definidos.

Con base a COBIT se han reestructurado normas que se centran en procesos específicos de las empresas y al pasar el tiempo hacen parte de los pilares fundamentales que mantienen un buen proceso de un gobierno corporativo, un gobierno TI y por ultimo un gobierno de seguridad de la información. (Ver figura 7)

5.2 ISO 27000

Figura 7: Normas de la información.



Fuente: Adaptado de “http://www.ieee.org.ar/downloads/2006-hrabinsky-itil.pdf”

La ilustración (ver fig. 7) muestra en formas generales algunas normas que se pueden llegar aplicar en algunos procesos y en su defecto en las dependencias de la organización, ya que estas normas siempre buscan un solo objetivo, ser competitivos en el mercado, partiendo de este punto la necesidad de manejar la información se hace cada ves la prioridad del negocio, pero cada paso que damos al futuro un nuevo reto se convierte en la segundad prioridad paralela para las TI y es denominado el gobierno de seguridad TI (Ver fig. 4, 7), este gobierno debe ser planeado antes, durante y después de definir las TI que se encuentran en la empresa, debido que la forma y herramientas utilizadas para realizar delitos informáticos no se han quedado atrás en la evolución de la tecnología, por tanto es de vital importancia aplicar métodos, políticas, procesos, objetivos, controles y un sin numero de elementos que nos permita blindar nuestros SI.

ISO 27000 (International Organization for Standardization) “Esta norma ha sido elaborada para brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento *y* mejora de un sistema de gestión de seguridad de la información (SGSI).”[11]

La implementación de un SGSI es recomendado para las organización y ser incluido en la estrategia de negocio, este debe ser diseñado teniendo en cuenta los objetivos, estrategias y direccionamiento de la empresa, sus alcances deben estar acordes con los requisitos de seguridad, los procesos empleados y la magnitud de la estructura organizacional, de esta manera se espera que un SGSI de soluciones acordes con la inversión realizada y que sea coherente con el tamaño del negocio un ejemplo de esto es “una situación simple requiere una solución de SGSI simple”

La norma se basa en procesos, de esta forma pretende establecer, operar, hacer seguimiento, mantener y mejorar el SGSI de la organización, la norma considera como un proceso “cualquier actividad que use recursos y cuya gestión permita la

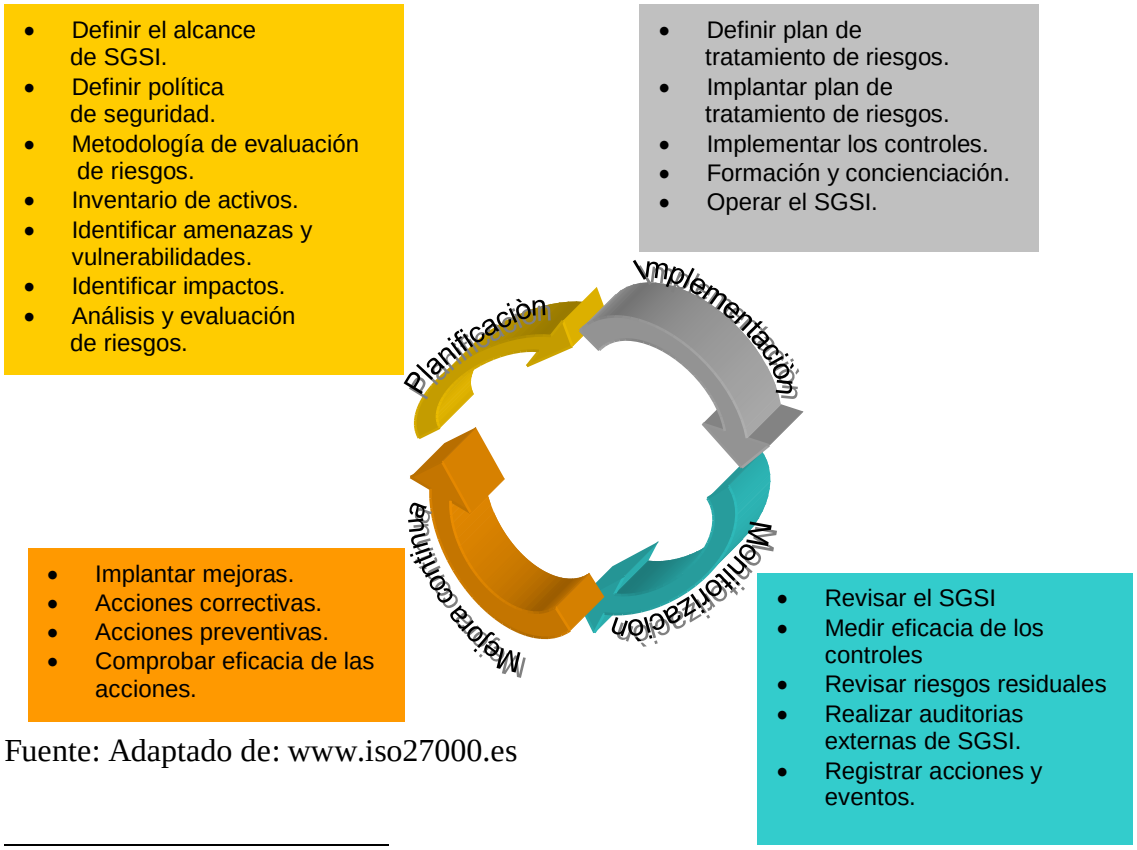
[11] ICONTEC, COMPENDIO Sistema de Gestión de la Seguridad de la Información. (SGSI). p.13.

transformación de entradas en salidas Con frecuencia, el resultado de un proceso constituye directamente la entrada del proceso siguiente."[12] El enfoque basado en procesos estimula a sus usuarios a hacer énfasis en la importancia de:

"a) Comprender los requisitos de seguridad de la información del negocio y la necesidad de establecer la política y objetivos en relación con la seguridad de la información;
b) Implementar y operar controles para manejar los riesgos de seguridad de la información de una organización en el contexto de los riesgos globales del negocio de la organización;
c) El seguimiento y revisión del desempeño y eficacia del SGSI
d) la mejora continua basada en la medición de objetivos." [13]

Partiendo de estos principios la norma nos presenta 4 pasos a seguir. (Ver. Fig. 8).

Figura 8: Norma ISO 27000



Fuente: Adaptado de: www.iso27000.es

[12] Ibid. p. 13.
[13] Ibid. p. 13.

Hoy día la norma ha tenido una excelente aceptación y eso se demuestra en mas de dos mil organizaciones se han certificado ISO 27000, esto nos deja ver la evolución de la administración de los recursos que se tiene en las organizaciones y como estos deben interactuar eficaz y eficientemente orientados a un mismo objetivo en común la competitividad mundial. A continuación se mencionan las empresas que colaboraron en el estudio de la norma[14]:

- *AV VILLAS*
- *ASOCIACIÓN BANCARIA DE COLOMBIA.*
- *BANCO CAJA SOCIAL / COLMENA BCSC*
- *BANCO GRANAHORRAR*
- *BANCO DE LA REPÚBLICA*
- *BANISTMO*
- *COLSUBSIDIO*
- *D.S. SISTEMAS LTDA*
- *FLUIDSIGNAL GROUP SA*
- *IQ CONSULTORES*
- *IQ OUTSOURCING SA*
- *MEGABANCO*
- *NEW NET SA*
- *SOCIEDAD COLOMBIANA DE ARCHIVISTAS*
- *UNIVERSIDAD NACIONAL DE COLOMBIA*
- *ETB S.A. ESP*

La norma se puso a consideración de las siguientes empresas:

- *ABN AMRO BANK*
- *AGENDA DE CONECTIVIDAD*

[14] Ibid. p. 12.

- *AGP COLOMBIA*
- *ALPINA SA*
- *ASESORIAS EN SISTEMATIZACION DE DATOS S.A.*
- *ASOCIACIÓN LATINOAMERICANA DE PROFESIONALES DE SEGURIDAD INFORMATICA DE COLOMBIA*
- *ATH*
- *BANCAFÉ*
- *BANCO AGRARIO DE COLOMBIA*
- *BANCO COLPATRIA RED MULTIBANCA COLPATRIA*
- *BANCO DAVIVIENDA*
- *BANCO DE BOGOTÁ*
- *BANCO DE COLOMBIA*
- *BANCO DE CRÉDITO*
- *BANCO DE CRÉDITO HELM FINANCIAL SERVICES*
- *BANCO DE OCCIDENTE*
- *BANCO MERCANTIL DE COLOMBIA*
- *SANCO POPULAR*
- *BANCO SANTANDER COLOMBIA*
- *BANCO STANDARD CHARTERED COLOMBIA*
- *BANCO 5UDAMERIS COLOMBIA*
- *BANCO SUPERIOR*
- *BANCO TEQUENDAMA*
- *BANCO UNIÓN COLOMBIANO*
- *BANK BOSTON*
- *BANK OF AMERICA COLOMBIA*
- *BSVA BANCO GANADERO*
- *BFR SA*

CENTRO DE APOYO A LA TECNOLOGIA INFORMATICA –CATI

Las empresas anteriores no son las únicas donde se puso a consideración la norma se aconseja ver la norma ISO 27000 (COMPENDIO Sistema de gestión de la seguridad de la información)[15], vale la pena aclarar que las empresas mencionadas algunas están en proceso de certificación y otras ya certificadas.

5.3 RIESGO INFORMATICO.

Uno de los grandes objetivos de la seguridad de la información es definir e implantar una metodología que permita detectar, analizar y controlar el riesgo o en su defecto mitigar la posibilidad que este ocurra en la organización. La norma técnica Colombiana NTC 5254[16] es una "guía para el establecimiento e implementación en el proceso de administración de riesgos involucrando el establecimiento del contexto y la identificación, análisis, evaluación, tratamiento, comunicación y el monitoreo en curso de los riesgos."[17] La norma define el riesgo como "la oportunidad que suceda algo que tendrá impacto en los objetivos."[18]

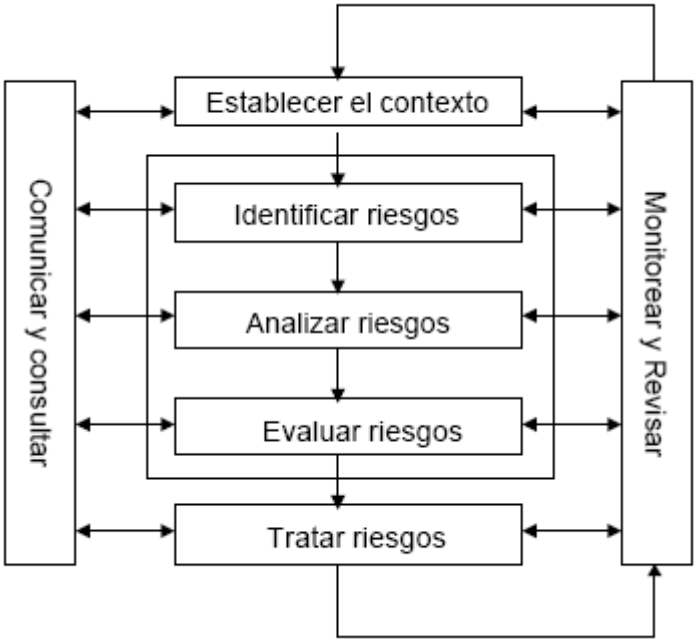
Administrar el riesgo trae consigo definiciones que se deben tener en cuenta para la correcta valoración del riesgo, estas definiciones son importantes procesos que varían de acuerdo con la metodología que la organización defina implantar sin dejar atrás la estructura organizacional de la compañía y las TI, algunas de estas definiciones son[19]:

- *Aceptación del riesgo: decisión de asumir el riesgo.*
- *Análisis del riesgo. Proceso sistemático para entender la naturaleza del riesgo y deducir el nivel del riesgo.*
- *Consecuencia. Resultado o impacto de un evento.*

[15] Ibid. p. 12.
[16] ICONTEC, RESUEMEN NORMA TECNICA COLOMBIANA NTC 5254. Colombia: ICONTEC 2006. p. 1.
[17] Ibid. p. 1.
[18] Ibid. p. 2.
[19] Ibid. p. 1.

- *Control. Proceso, política, dispositivo, práctica u otra acción existente que actúa para minimizar el riesgo negativo o potenciar oportunidades positivas.*
- *Evaluación del control. Revisión sistemática de los riesgos para garantizar que los controles aún son eficaces y adecuados.*
- *Evento. Ocurrencia de un conjunto particular de circunstancias.*
- *Frecuencia. Medición del número de ocurrencias por unidad de tiempo.*
- *Posibilidad. Se usa como descripción general de la probabilidad o la frecuencia.*
- *Monitorear. Verificar, supervisar o medir regularmente el progreso de una actividad, acción o sistema para identificar los cambios en el nivel de desempeño requerido.*
- *Probabilidad. Medida de la oportunidad de ocurrencia expresada como un número entre 0 y 3.*
- *Riesgo residual. Riesgo remanente después de la implementación del tratamiento del riesgo.*
- *Valoración del riesgo. Proceso total de identificación, análisis y evaluación del riesgo.*
- *Criterios del riesgo. Términos de referencia mediante los cuáles se evalúa la importancia del riesgo.*
- *Reducción del riesgo. Acciones que se toman para reducir la posibilidad y consecuencias asociadas a un riesgo.*

Figura 9. Elementos que conforman el proceso de gestión del riesgo.



Fuente: http://www.gitltda.com/estandares.html

5.3.1 PROCESO DE LA GESTIÓN DE RIESGO.[20]

Comunicación y consulta: Es necesario la capacitación del personal que participara en la elaboración de los riesgos ya que debe tener el conocimiento amplio para la gestión y planeación del riesgo. Además la comunicación con las dependencias internas o externas es fundamental para la detección efectiva de los riesgos existentes.

Establecer el contexto: se enmarca en el tipo de ambiente que rodea la administración del riesgo, contemplando diferentes varíales que juegan un papel importante como: El tipo de negocio, reglas existentes en la seguridad de la información, financiero, político, oportunidades y amenazas.

[20] Ibid. p. 3-7.

Identificar los riesgos: ¿que puede suceder?, ¿por qué? (causas) y las consecuencias, que conforma un proceso ya sea interno o externo, ¿que impide alcanzar un objetivo?

Analizar el riesgo: consiste en entender el riesgo, cuales son sus alcances y de que forma se puede controlar teniendo en cuenta los costos, que resultados tendría la solución y que tan probable seria el riesgo.

Evaluar el riesgo: es el resultado del análisis del riesgo teniendo en cuenta el contexto.

Tratamiento de los riesgos: consiste en identificar que opciones existen para tratar el riesgo, teniendo en cuenta la planeación e implementación.

Monitoreo y revisión: una revisión constante a los riesgos, plan de riesgos y la implementación de los controles, disminuirá de forma preventiva el riesgo.

5.4 Políticas de seguridad informática.

Las políticas de seguridad son ITEMS fundamentales que permiten la comunicación sencilla del buen uso de las herramientas y sistemas de información que la organización posee. Dando a conocer las buenas prácticas del manejo de la información, resaltando siempre la integridad del los sistemas, ratificando que la información es el eje fundamental de la organización. Se debe tener en cuenta algunos elementos importantes para la elaboración de las políticas:[21]

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.

[21] JEIMY, C. (2000) Políticas de Seguridad Informática. http://www.criptored.upm.es/guiateoria/gt_m142a.htm

- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.
- Definición de violaciones y de las consecuencias del no cumplimiento de la política.
- Responsabilidades de los usuarios con respecto a la información a la que el o ella tiene acceso.

Las políticas deben surgir a partir del análisis y administración del riesgo, deben ser claras y especificar quien es la autoridad que asuma las medidas disciplinarias y evaluación de la situación, estas deben ser promovidas y dadas a conocer a todos los empleados.

6. DESARROLLO DEL PLAN DE ACTIVIDADES

6. 1 Alcance:

Aumento en la administración y gestión de la seguridad de la información aplicando en la norma ISO 27000 en la subgerencia de Informática y Tecnología, delimitada en las funciones de la administración de la base de datos, desarrollo del software corporativo y administración de la red corporativa, incluyendo en este proceso leyes y normas que exijan los entes auditores de TELEBUCARAMANGA.

6.2 Observaciones preliminares.

- La subgerencia de informática no cuenta con un documento oficial que defina el sistema de gestión de la seguridad de la información, pero en su defecto tiene documentos individuales que contienen parámetros que reflejan la administración de la seguridad de la información.
- La dependencia cuenta con un documento que recopila las políticas corporativas, además tiene definido formatos y procesos que respaldan este documento.
- La organización ha implementado la norma NTC 5254 (Norma Técnica Colombiana de Gestión de Riesgos) Cuenta con auditorias internas y externas que evalúan constantemente el riesgo y generan documentos con sus recomendaciones. También existe un plan de contingencia diseñado específicamente para Telebucaramanga.
- La subgerencia diseño un sistema de información que permite administrar (características, tipo, ubicación, responsable, cantidad, entre otras.) todos los activos de la organización.

6.3 Políticas de seguridad de la información.

La política de seguridad definida por la empresa esta basada en las estrategias del negocio, activos de la organización, ubicación, requisitos del negocio, legales o reglamentarias. *(Ver anexo A.)*

6.4 Amenazas y vulnerabilidades en el manejo de la información.

Telebucaramanga cuenta con planes contingentes referentes a:

- Suspensión de la energía en el centro de cómputo, sedes administrativas y operativas.
- Inundaciones en el centro de cómputo, sedes administrativas y operativas.
- Incendios en el centro de cómputo, sedes administrativas y operativas.
- Contingencia al no acceso a la sede de la empresa (Paros sindicales).
- Terremotos / bombas en el centro de cómputo, sedes administrativas y operativas.
- Contingencia a daños hardware y software.

Por esta razón en la tabla de Amenazas y vulnerabilidades se mencionarán los temas anteriores de forma general. Se recomienda Ver anexos D,E,F,G,H y I.

6.4.1 Niveles De Impacto:

TABLA 1: Niveles de impacto

Asignados en la tabla están regidos por la norma NTC 5254 (Norma Técnica Colombiana de Gestión de Riesgos)	
Si el impacto no afecta de manera significativa y puede ser asumido por el giro normal de las operaciones del prestador ya que no afecta la operación del servicio, la viabilidad empresarial o la relación con el usuario, los efectos (operativos, financieros, de imagen, etc.) sobre la empresa al ocurrir este evento son menores.	5

Se puede ver afectada la eficiencia del prestador disminuyéndose la calidad del servicio, generando insatisfacción en el usuario y retrasos en la operación, en este caso los efectos son importantes	10
Si los efectos son mayores cuando se afectan los estándares de los indicadores, se generan incumplimientos regulatorios, se puede poner en riesgo la prestación del servicio, la viabilidad empresarial y se afecta la relación con el usuario.	20

TABLA 2: AMENAZAS Y VULNERABILIDADES				
AMENAZA	FUENTE DE LA AMANEZA	VULNERABILIDAD	QUE HACER	IMPACTO
Centro de computo				
Suspensión de la energía.	Problemas con la Electrificadora.	El sistema de información queda fuera de servicio. Daños en el hardware.	Se cuenta con dos UPS en cascada y Baterías secas para la misma que le permiten una autonomía de 30 minutos de carga plena. Además se cuenta con una planta de energía de respaldo a las UPS.	20
Inundación	Ruptura de tubo de agua.	Daños en la Infraestructura del centro de cómputo. Modificación y/o destrucción de la Información. Humedad y/o filtraciones de agua.	Las tuberías cercanas al centro de cómputo deben ser cubiertas. Revisar periódicamente por el personal de mantenimiento las tuberías.	20

Incendio	Presencia de un incendio en el centro de cómputo	Daños en la Infraestructura del centro de cómputo. Modificación y/o destrucción de la Información.	Implementar un sistema automático de detección y extinción de incendios, garantizar contratos de Mantenimiento. Instalar extintores en el centro de cómputo que puedan ser utilizados para pequeños incendios.	20
Paros sindicales	Impedimento de ingreso del personal por el sindicato.	Manipulación de la información. Centro de cómputo sin atender.	Operación de consolas remotas. Activación de maquinas de respaldo.	20
Terremoto / bomba	Terrorismo o terremoto.	Daño físico al edificio. Destrucción los servidores.	Implementar el plan de contingencia ante desastres. Maquinas externas de respaldo.	20

Violación de seguridad física.	Acceso de personal no autorizado. Personal autorizado con diferencias personales con la empresa.	Alteración, divulgación o destrucción de la información. Robo de componentes hw.	Se tiene vigilancia externa las 24 horas Implementar un sistema de acceso de personal autorizado y no autorizado.	20
Violación de la seguridad lógica.	Conocimiento de las claves se acceso por personal no autorizado.	Uso del perfil de usuario por personal Alteración, divulgación o destrucción de la información.	No dejar ventanas abiertas en las estaciones de trabajo si el operador no se encuentra. El personal que no realice trabajos especiales debe ser retirado.	20

AMENAZA	FUENTE DE LA AMANEZA	VULNERABILIDAD	QUE HACER	IMPACTO
TABLA 3: Comunicaciones				
Suspensión de la energía.	Falla de energía eléctrica en el switch principal.	Falla de switch que conecta todos los servidores y el enlace de red. Daño del hardware en el switch.	Monitorear el funcionamiento del tráfico del switch con software adquirido por la empresa. Aplicar la contingencia diseñada.	10
Fallas de equipos.	Daños en la tarjeta o cualquier dispositivo interno del switch.	Falla de switch que conecta todos los servidores y el enlace de red.	Monitorear el funcionamiento del tráfico del switch con software adquirido por la empresa. Verificar el estado de garantía de los equipos.	10
	Manipulación incorrecta de los equipos.	Fallas de un nodo que sacaría a las oficinas que están en dicho nodo.	Capacitar a los operadores constante mente. Seguir las indicaciones de los procedimientos documentados.	20
	Alta densidad de partículas de polvo al interior de los equipos que degraden los componentes.	Fallas en los equipos. Podría afectar el buen funcionamiento del sistema de información.	Mantenimiento preventivo de los equipos. Implementar el plan de contingencia ante fallas hardware diseñado por la compañía.	10

Fallas de software.	Configuración incorrecta de la red.	Dejar sin servicio las oficinas conectadas a un nodo o en su defecto toda la red.	Revisar los procedimientos definidos por el área de sistemas para realizar dichas configuraciones.	10
	Cambios no autorizados en la configuración de la red.		Los administradores de la información (red, dba.) son los únicos que pueden manipular las configuraciones correspondientes al SI. Revisar las políticas de seguridad.	20
	Mala capacitación de los administradores de la información.		Capacitación constante de los administradores de la información.	
Fallas de conexiones.	Ruptura de las conexiones de fibra que van al backbone principal.	Caída del SI de los nodos afectados o en su defecto todo el SI de la compañía.	Monitoreo preventivo de las redes y reportes de daños. Revisar la contingencia de daños físicos en la red.	20
	Fallas de los puertos de los switches.		Monitoreo preventivo de los nodos y limpieza de estos.	10
Violación de seguridad física.	Manipulación de equipos por personal no autorizado.	Falla de switch que conecta todos los servidores y el enlace de red.	Verificación de los controles de acceso a las oficinas de cómputo.	20

AMENAZA	FUENTE DE LA AMANEZA	VULNERABILIDAD	QUE HACER	IMPACTO
TABLA 4: servidores				
Fallas de hardware.	Variación de voltaje.	No disponibilidad de la maquina.	Equipos conectados a energía regulada.	20
	Falla de la fuente de poder.		Remplazar la fuente de poder. Implementar la contingencia de daños físicos.	10
	Condiciones ambientales.		Equipos con aire acondicionado.	20
	Fallas de los discos duros.	Perdida de información.	Remplazar el disco. Implementar la contingencia de daños físicos. Contrato de mantenimiento con firma especialista.	20
	Falla en la tarjeta de red.	Perdida de conexión total de la maquina.	Remplazar de la tarjeta. Monitoreo de fallas a través de un LOG del sistema.	10
	Falla en el cableado o equipos de comunicación.		El equipo de soporte debe estar disponible 7 * 24	10
Fallas de software.	Mala configuración del sistema por los administradores de la información.	No disponibilidad de la maquina.	Capacitación constante de los administradores de la información. Revisar procesos ya definidos	20

			de la configuración de los equipos.	
seguridad	Mala configuración de la seguridad de la maquina y/o de la red. Nuevas técnicas de delitos informáticos.	Alteración, divulgación o destrucción de la información.	Implementación y/o revisión de las políticas de seguridad. Capacitación de nuevas técnicas de seguridad de la información.	

6.5 Metodología de evaluación de riesgos.

Telebucaramanga es una compañía que es supervisada por todos los entes auditores del estado; por ello el "Departamento Administrativo de la Función Pública" adapta la norma técnica Colombiana NTC 5254 a las necesidades de Telebucaramanga. *(Ver anexo B.)*

6.6 Normatividad de la seguridad de la información.

(Ver anexo C.).

7. Análisis corporativo.

Si bien es cierto que la subgerencia de informática y tecnología es una dependencia estable, con personal capacitado, que maneja en su infraestructura tecnológica una homogeneidad y ha logrado mantener una estabilidad del sistema de información y de todos los recursos informáticos que ella administra, es de suma importancia resaltar que no cuenta con el recurso humano suficiente para realizar otras labores de administración de red, como investigación y monitoreo diario de la seguridad de la información de la compañía, gestión y actualización de la documentación de los desarrollos software y de la plataforma hardware de la organización. Esta falta de recurso humano en la subgerencia ha obligado que no sean segregadas las funciones de manera adecuada en las áreas de crecimiento informático y gestión infraestructura de procesamiento.

Ejemplo de ello es la falta de respaldo humano capacitado en la ausencia del dba de la compañía, aunque los procesos, accesos a medios físicos y lógicos se encuentran documentados no se dispone de un perfil profesional con experiencia que asuma total responsabilidad y confiabilidad la administración de las labores del cargo, resaltando de manera categórica que las funciones de la administración de red son funciones actuales del mismo y se cuenta con un solo operador en la gestión backup y soporte de primer nivel del data center.

La subgerencia se ha esforzado en la adquisición de herramientas que garanticen la estabilidad de los sistemas de información que esta maneja, con componentes tecnológicos robustos como una base de datos ORACLE y la herramienta de desarrollo Developer, configuradas en servidores Sun Microsystems, trabajando en el sistema operativo Solaris, a nivel de red se cuenta con un servidor IBM bajo un ambiente Novell Netware y el 90% de las estaciones de trabajo marca DELL

con excelentes características técnicas. Se recomienda leer las conclusiones y recomendaciones para reforzar este análisis corporativo.

8. Conclusiones.

La Subgerencia de Informática y Tecnología no cuenta con un comité responsable de la seguridad de la información, que estructure un plan estratégico encaminado a proteger los activos de la empresa, encargado de la definición, documentación, implementación y actualización de las políticas, los controles, amenazas, vulnerabilidades y riesgos de la información, que gestione la investigación e implementación de nuevas tecnologías, direccionando el sistema de gestión de la seguridad de la información corporativa.

La Subgerencia de Informática y Tecnología no cuenta con el personal suficiente para realizar labores de administración de red y solo cuenta con un operador de Help Desk, en consecuencia de esto el administrador de la base de datos es el encargado de asumir las funciones de la administración de la red y la seguridad de la plataforma tecnológica a cargo de la subgerencia, resaltando de manera categórica que no se dispone de una persona que sirva como backup del “DBA” de la empresa, que asuma total responsabilidad y confiabilidad las funciones del cargo.

Actualmente la Subgerencia de Informática y Tecnología no cuenta con servidores de respaldo para los servicios de red, correo corporativo, intranet y conexionas remotas de la organización. Asumiendo en algunas eventualidades soluciones que no son las óptimas y que generan inconformidad en la continuidad del servicio. Resaltando que en el servidor de red se encuentran definidos los perfiles de cada usuario de la compañía y en una eventual falla no se podría tener acceso a la información de una manera controlada, siendo este un servidor robusto la solución seria demorada, afectando la continuidad eficiente del servicio.

La Subgerencia de Informática y Tecnología cuenta con la documentación, el conocimiento y las herramientas básicas para llevar cabo la implementación formal de la norma ISO 27000, incluyendo en la culminación de esta etapa los controles que la misma norma recomienda para lograr la certificación, sin dejar a un lado los diseños e investigaciones de otras normas que las auditorias tanto externas como internas proponen y en algunas ocasiones exigen.

9. Recomendaciones

Se recomienda definir un comité responsable de la seguridad de la información que garantice la disponibilidad, integridad, confidencialidad y auditabilidad de la misma, además no existe un cronograma específico orientado a la investigación e implantación de nuevas herramientas que gestionen la seguridad de la información.

Se recomienda definir un cronograma de actividades dirigido a la actualización, revisión y control de políticas de seguridad, amenazas, vulnerabilidades, nuevos riesgos y toda la documentación que el sistema de gestión de la seguridad de la información exija.

Se recomienda la realización de campañas de concientización y formación al personal de la empresa en materia de la seguridad de la información, donde se refuercen las actualizaciones de las políticas de seguridad, el buen manejo de los dispositivos tecnológicos al servicio de los usuarios, las diferentes penalizaciones corporativas acordes con la ley y los deberes de empresa en los temas anteriormente mencionados. Cabe la pena resaltar que este tipo de programas deben ser manejados con el apoyo de Gestión Humana y el cronograma de actividades debe estar aprobado por el comité se seguridad de la información.

Se recomienda actualizar paulatinamente el cableado estructurado de la compañía de categoría 5 a la categoría 6, ya que a futuro el medio de comunicación no puede ser un obstáculo en la implementación de nuevas tecnologías.

En el mercado tecnológico existen nuevas soluciones que permiten mejorar el redimiendo, continuidad del servicio y el respaldo ante eventualidades que puedan llegar a perjudicar la estabilidad del negocio. Si bien es cierto que los servidores actuales de la plataforma tecnológica de la empresa trabajan de forma estable se recomienda evaluar nuevas propuestas que permitan la actualización de la infraestructura del data center, justificada esta recomendación en equipos principales adquiridos del año 98, 2000 / 2003, la no existencia de servidores de respaldo para la red, correo corporativo, intranet, conexionas remotas y nuevas soluciones que presentan los proveedores de hardware y software.

Teniendo en cuenta la departamentalización por dependencias de la empresa, la infraestructura tecnológica y el número de usuarios, el riesgo violación a la seguridad de la información es considerable, partiendo de estas razones es recomendable la implementación de redes virtuales ya que permiten segmentar de forma adecuada y ordenada la administración de la red. Actualmente la empresa presenta en algunas ocasiones conflicto de IP's y transferencias de archivos compartidos sin autorización entre dependencias.

Es recomendable desagregar las funciones de administración de la red, administración de la base de datos, gestión y administración de la seguridad de la información ya que por gestión y seguridad no es recomendable que estas tres funciones sean realizadas por una sola persona.

Se recomienda gestionar en las funciones del administrador de la seguridad de la información monitoreo constante de la red corporativa, generación de estadísticas de rendimiento, investigación y propuestas de nuevas implementaciones que permita garantizar el servicio continuo y optimo de la plataforma de red.

10. BIBLIOGRAFIA

ICONTEC, COMPENDIO Sistema de Gestión de la Seguridad de la Información. (SGSI). Colombia: ICONTEC 2006.

ELISSONDO, Luis. Auditoría y Seguridad de Sistemas de Información. Disponible en: http://200.5.106.140/academicas/catedras/Seguridad%20y%20Control%20Informatico/AS_COBIT.ppt

Capítulo Argentino de la IEEE Computer Society. Disponible en: http://www.ieee.org.ar/downloads/2006-hrabinsky-itil.pdf

ARBELÁEZ, Roberto. CXXVI Salón de INFORMÁTICA. Disponible en: http://www.acis.org.co/fileadmin/Base_de_Conocimiento/XXVI_Salon_Informatica/RobertoArbelaezXXVISalon2006.pdf

Bernal, Luis Miguel. Gerente de servicios de campo de Getronics. Disponible en: http://www.dinero.com/wf_InfoArticulo.aspx?IdArt=36450

LEONARDO, S Y SIMONT. (2004) Introduccion al riesgo informatico. Disponible en: http://www.audisis.com/Audideas%209_6.htm

JEIMY, C. (2000) Políticas de Seguridad Informática. Disponible en: http://www.criptored.upm.es/guiateoria/gt_m142a.htm

ANEXOS

ANEXO A: Políticas de seguridad informática Telebucaramanga.

POLITICAS DE SEGURIDAD INFORMATICA TELEBUCARAMANGA

Se define este documento como directriz y guía para la aplicación de acciones y controles tendientes a garantizar un buen nivel de seguridad sobre la plataforma informática de TELEBUCARAMANGA, se estructura de manera clara, sencilla y totalmente ajustado a la Empresa para facilitar su total aplicabilidad

I

POLITICA: Se desactivan las unidades de acceso para cd-rom y diskette, a fin de prevenir la instalación de software no autorizado y/o la entrada de virus por estos medios, solamente se activan previa firma electrónica o física del convenio de activación.

ADMINISTRACION: El personal de soporte a usuarios es el encargado de realizar la configuración de las máquinas, el Administrador de la red debe definir una política a nivel del servidor para inhibir el acceso a estos medios

REVISION: Dos veces al año, se verifica la instalación de software no autorizado, en caso de presentarse infección por virus, se hará el seguimiento respectivo a fin de determinar la causa del mismo y el nivel de incumplimiento del acuerdo firmado. Es también causal de penalización la activación mediante medios alternos de las unidades sin la firma previa del convenio de activación.

PENALIZACION: La Subgerencia de Informatica y Tecnología informará por escrito electrónico o físico a la Direccion de Gestion Humana sobre el hallazgo de cualquiera de las infracciones a la política y esta Dirección se encargará de aplicar las sanciones que apliquen.

II

POLITICA: Todos los equipos de la red tendrán instalado software antivirus con actualizaciones del motor de detección no superior a una semana, adicionalmente toda información referente a virus se canalizará por la Subgerencia Informática y Tecnología para verificar su validez antes de darla a conocer a todo el personal.

ADMINISTRACION: La Subgerencia Informática y Tecnología contará con un contrato de mantenimiento que le permita contar con las últimas versiones del software antivirus.

El administrador de la red será el encargado de descargar periódicamente (mínimo una vez por semana), los upgrade de la base de datos de escaneo, también debe definir una política y proveer en la red los agentes e instaladores del producto antivirus.

Soporte a Usuarios se encargará de la instalación inicial del antivirus en las máquinas cliente, teniendo en cuenta la capacidad hardware de los microcomputadores y tratando al máximo de afectar lo menos posible el desempeño general del equipo con la porción residente del antivirus.

El Subgerente informará a todos los usuarios que se debe comunicar cualquier altera de virus inicialmente a la Subgerencia de Informática y Tecnología antes de difundirla a todos los demás usuarios, el Administrador LAN verificará la validez de la alerta con el proveedor a fin de aplicar las acciones requeridas y difundirlo a todos los usuarios de la red si aplica.

REVISION: En caso de infección se hará la revisión por parte de soporte a usuarios a fin de determinar si los productos están instalados o si han sido removidos manualmente los agentes o sus ejecutables.

PENALIZACION: Las sanciones a aplicar dependerán del daño ocasionado por el virus y el nivel de infección causado tanto en la máquina origen como en los demás equipos infectados.

III

POLITICA: Se restringirá el acceso de los equipos cliente a la opción RED del panel de control, archivo de registro de Windows y propiedades del cliente Novell a fin de evitar alteraciones en la configuración de los equipos.

ADMINISTRACION: El administrador de la red debe implementar esta política en el servidor y aplicarla a todos los usuarios a excepción de los funcionarios de la Subgerencia de Informática y Tecnología y soporte de la red multiservicios.

REVISION: En caso de desconfiguración en cualquier máquina, el área de soporte a usuarios hará un diagnóstico a fin de determinar la falla, reforzando la política y el nivel de responsabilidad del cliente.

PENALIZACION: Llamado de atención al usuario si aplica, a fin de concientizarlo de la pérdida de tiempo ocasionada para él y para el personal técnico por el incumplimiento de esta política.

IV

POLITICA: El acceso a Internet se hará en horarios preestablecidos previo diligenciamiento electrónico o físico y autorización del Jefe inmediato con el formato ACCESO A INTERNET, teniendo claro que su uso se debe hacer exclusivamente para efectos labores, quedando expresamente prohibido el acceso a páginas pornográficas, de entretenimiento, descarga e instalación de software no autorizado.

ADMINISTRACION: El administrador LAN implementará los horarios de acceso y los asignará a los usuarios que lo requieran con el formato antes mencionado, Soporte a usuarios habilitará el browser en cada equipo a fin de permitir la navegación.

REVISION: El administrador LAN mensualmente elaborará un reporte de visitas a páginas prohibidas e inhibirá el acceso a dichas páginas a fin de evitar su consulta posterior por parte de otros usuarios, e informará al Subgerente IT a fin de iniciar la aplicación de los correctivos fijados en penalización.

PENALIZACION: En caso de comprobarse el acceso a páginas prohibidas se hará un llamado de atención al usuario por parte del Subgerente de Informática y Tecnología, si se presenta reincidencia se suspenderá el servicio de navegación por un mes, si se presenta una nueva reincidencia se suspenderá definitivamente el servicio y se enviará comunicación a recursos humanos.

V

POLITICA: Los usuarios de Telebucaramanga que diligencien el formato de acceso a la red tendrán acceso al correo corporativo, los contratistas deberán solicitar éste por aparte, y en cualquier caso el uso de este servicio será solamente para efectos laborales, quedando expresamente prohibido su uso para mensajes pornográficos o de entretenimiento, adicionalmente el buzón y archivos adjuntos tendrá un tamaño límite y es responsabilidad del usuario mantener estos límites para permitir el normal funcionamiento del servicio.

ADMINISTRACION: El administrador LAN crea la cuenta y el área de soporte a usuarios realiza la instalación de la porción cliente del software de correo.

REVISION: En caso de recibir reporte de manejo de información prohibida por el correo electrónico, se hará una revisión sin previo aviso del buzón denunciado en presencia del usuario a fin de verificar el contenido prohibido, en caso de comprobarse se hará un llamado de atención y la advertencia de la posibilidad de cambios no avisados de contraseña a fin de verificar el incumplimiento de esta política y aplicar las penalizaciones.

PENALIZACION: Si se comprueba el uso indebido del correo se hará un llamado de atención, en caso de reincidencia se suspenderá el servicio por un mes y por una tercera falla se retirará de manera definitiva con comunicación a la Dirección de Recursos Humanos

VI

POLITICA: El acceso a la Red Corporativa de Telebucaramanga se hace mediante el diligenciamiento físico o electrónico del formato ACCESO A LA RED (anexo 5)

ADMINISTRACION: En la intranet se dispondrá una página en la cual el Jefe Inmediato solicitará el acceso a cada uno de los SISTEMAS DE INFORMACION, acto seguido el Administrador LAN creará el usuario e informará a soporte a usuarios para que asesoren al funcionario en su primera conexión.

REVISION: En caso de accesos a información clasificada como confidencial (Anexo 6) se solicitará el visto bueno a Auditoría Interna quienes validarán el requerimiento real de acceso a dicha información.

En caso de daño, eliminación o difusión de información se comunicará el insuceso a Auditoría Interna para que adelante la investigación requerida.

PENALIZACION: Una vez definido el nivel de responsabilidad del usuario por daño, eliminación o difusión de información se aplicarán las sanciones contempladas en reglamento interno de trabajo.

VII

POLITICA: El acceso a las aplicaciones corporativas se hace mediante el diligenciamiento físico o electrónico del formato ACCESO A SISTEMAS DE INFORMACION (Anexo 7)

ADMINISTRACION: En la intranet se dispondrá una página en la cual el Jefe Inmediato solicitará el acceso a cada uno de los recursos de red, acto seguido el

Administrador LAN creará el usuario e informará a soporte a usuarios para que asesoren al funcionario en su primera conexión.

REVISION: En caso de accesos a información clasificada como confidencial (Anexo 6) se solicitará el visto bueno a Auditoría Interna quienes validarán el requerimiento real de acceso a dicha información.

En caso de daño, eliminación o difusión de información se comunicará el insuceso a la Dirección de Auditorías para que adelante la investigación requerida.

PENALIZACION: Una vez definido el nivel de responsabilidad del usuario por daño, eliminación o difusión de información se aplicarán las sanciones contempladas en reglamento interno de trabajo.

VIII

POLITICA: Todo el software instalado en TELEBUCARAMANGA, cumplirá los lineamientos de licenciamiento fijados para cada caso, cumplimiento con la legislación que para el momento se encuentre vigente.

ADMINISTRACION: El área de soporte usuarios hará el registro del software y hardware adquirido a fin de mantener un inventario vigente de las licencias instaladas y licenciadas y verificar la necesidad de adquisición.

REVISION: Semestralmente se hará un recorrido máquina por máquina chequeando el software instalado a fin de verificar su origen y licenciamiento, actualizando el inventario y definiendo niveles de responsabilidad de los usuarios.

PENALIZACION: En caso de hallazgo de software no autorizado y teniendo en cuenta la gravedad de la falta se informará al infractor con copia al Jefe Inmediato y se procederá a la desinstalación inmediata del producto, en caso de reincidencia se informará a Recursos Humanos a fin de aplicar las sanciones respectivas.

IX

POLITICA: La instalación, traslado y configuración de microcomputadores, elementos de red, servidores, periféricos y en general cualquier equipo de cómputo que se integre a la red corporativa de Telebucaramanga será realizada únicamente por personal de la Subgerencia IT.

ADMINISTRACION: La integración de cualquier elemento nuevo a nivel cliente será realizada por el área de soporte a usuarios, a nivel servidores y red por el administrador de red o base de datos según corresponda.

REVISION: En caso de comprobarse cualquier contravención a esta política por simple que esta parezca se hará un llamado de atención al funcionario implicado, a fin de hacerle entender las dificultades técnicas que puede tener el realizar estas labores sin el conocimiento global y el nivel de daño que ésto puede implicar.

PENALIZACION: Llamado de atención, en caso de reincidencia se informará al Jefe Inmediato y por una nueva reincidencia se informará a Recursos Humanos.

X

POLITICA: Las contraseñas para los usuarios finales a nivel de red y aplicaciones tendrán una longitud mínima de 6 caracteres, con vencimiento cada 2 meses, no hay posibilidad de reuso de claves, la clave debe empezar con letras, debe contener letras y números, debe diferir por lo menos en tres caracteres de la clave anterior.

ADMINISTRACION: Las aplicaciones y software de red deben permitir y validar el cumplimiento de la política.

REVISION: No aplica.

PENALIZACION: Se advertirá a los usuarios que cualquier acción realizada sobre la red que aparezca bajo su usuario es de responsabilidad exclusiva del usuario registrado por ello es crucial y de responsabilidad personal mantener las claves como confidenciales.

XI

POLITICA: Las contraseñas de los servidores, elementos de red y demás elementos compartidos (Anexo 8) serán de 8 caracteres o más, siempre serán letras o números que no conformen palabras, y se entregarán en sobre sellado al Subgerente IT cada dos meses, serán de conocimiento exclusivo del administrador responsable.

ADMINISTRACION: El administrador fija las contraseñas y luego las entrega en sobre cerrado al Director, este sobres solo será abierto en caso de imposibilidad de contacto con el administrador, es posible habilitar contraseñas temporales para uso por parte de otros funcionarios de la Subgerencia IT previa justificación de la necesidad y registro en la bitácora respectiva.

REVISION: Líder del Area de Recursos Informáticos Corparativos puede hacer revisiones esporádicas del cumplimiento de esta política.

PENALIZACION: En caso de incumplimiento se hará el llamado de atención a los administradores, si se presenta reincidencia se hará un llamado de atención por

escrito y por una tercera reincidencia se informará a la Dirección de de Recursos Humanos.

XII

POLITICA: El acceso a la sala de servidores es totalmente restringido y solo se permite al Subgerente IT, administrador de la base de datos, administrador de la red y líder del área de recursos informáticos, permitir el acceso a cualquier otro funcionario será responsabilidad de quien lo autoriza.

ADMINISTRACION: Se contará con puertas que permitan mediante cualquier medio el registro y control de entrada y salida a la sala de servidores.

REVISION: En caso de desconexión, daño, alteración, sustracción de cualquier elemento de la sala de servidores, la responsabilidad recaerá sobre quien haya accesado o permitido el acceso en el horario del insuceso, para lo cual se tendrá un registro automatizado de entradas y salidas.

PENALIZACION: El incumplimiento de esta política, acarreará sanciones dependiendo del nivel de gravedad del daño ocasionado a la infraestructura y serán impartidas por parte de recursos humanos.

XIII

POLITICA: La instalación de cualquier tipo de software en Telebucaramanga es función y responsabilidad exclusiva de la Subgerencia Informática y Tecnología.

ADMINISTRACION: El Administrador de la red en conjunto con el área de soporte a usuarios definirán y permitirán el acceso a los instaladores de los diferentes productos y mantendrán copias de los medios originales (anexo 9) de instalación en bóveda de seguridad.

REVISION: Cada vez que llegue un nuevo producto se debe definir y documentar claramente el proceso de instalación, dándolo a conocer al personal de soporte, se debe tratar al máximo de automatizar los procesos de instalación tendiendo a estandarizarlos para evitar soportes posteriores por instalaciones personalizadas, para lo cual se tendrá en cuenta los recursos hardware y la arquitectura que se maneje en el momento.

PENALIZACION: Se infringe esta política cuando personal de soporte haga instalaciones no autorizadas y/o facilite los medios para que un usuario final lo haga o cuando un usuario final realice instalaciones no autorizadas, en cualquiera de los dos casos se hará un llamado de atención al infractor.

XIV

POLITICA: Se tendrán bases de datos de trabajo para todas y cada una de las aplicaciones para permitir pruebas por parte del equipo de desarrollo, en ambientes separados al ambiente de producción y el acceso a los aplicativos será a nivel de consulta.

ADMINISTRACION: El administrador de la base de datos creará y mantendrá bases de datos de trabajo para el equipo de desarrollo, siendo su responsabilidad la actualización masiva de datos, afinamiento y cambios estructurales.

REVISION: Con frecuencias definidas para cada base de datos se hará una actualización de información, las contraseñas de acceso a estas bases pueden ser compartidas por los usuarios y manejar esquemas administrativos y de propietario para permitir pruebas integrales.

PENALIZACION: El realizar actualizaciones y/o pruebas en las bases de datos de producción hará acreedor de un llamado de atención al infractor o sanciones más drásticas en caso de daño superior o comprobarse intensión.

XV

POLITICA: Toda actualización, cambio, implementación, generación de información o mantenimiento a los sistemas de información debe hacerse con base en un soporte físico o electrónico que de acuerdo con el nivel de complejidad o efecto debe venir autorizado por el jefe inmediato.

ADMINISTRACION: Los ingenieros de soporte software actuarán con base en soportes físicos o electrónicos para realizar cambios a los objetos que componen las aplicaciones, autorizados por el Subgerente de IT en caso de que éstos ameriten.

REVISION: Esporádicamente el Subgerente o el líder del área de software pueden realizar una revisión de soportes.

PENALIZACION: En caso de daño, alteración, bloqueo o cualquier otra consecuencia efecto de un cambio realizado por el personal de desarrollo software del cual no exista soporte se adjudicará la responsabilidad al mismo y será éste quien asuma las consecuencias del hecho.

XVI

POLITICA: Los objetos software que componen los aplicativos deben tener esquemas de desarrollo y producción con acceso de lectura - escritura para el equipo de desarrollo sobre los primeros y de lectura para el personal que aplica sobre los segundos, solamente después de realizar pruebas se moverán los

objetos de producción a desarrollo, labor realizada por un único funcionario con privilegios de administración en la red.

ADMINISTRACION: El administrador debe crear áreas para los usuarios donde se tengan definidas las jerarquías que fija esta política (anexo 10).

REVISION: En caso de presentarse daño o pérdida sobre objetos software de las áreas de producción, ésto será responsabilidad del administrador de red, en caso de presentarse sobre los objetos de desarrollo se debe verificar el nivel de intención e impacto de las acciones realizadas, para lo cual se tendrá como base el histórico de modificaciones sobre los objetos.

PENALIZACION: De acuerdo con el nivel de daño y responsabilidad causado se aplicarán las sanciones que apliquen.

XVII

POLITICA: Todos los usuarios de la red corporativa que sean funcionarios de Telebucaramanga contarán con una unidad privada en el servidor de archivos, con un tamaño límite (anexo 4) para realizar el almacenamiento de la información y archivos que se consideren críticos y utilizarán este espacio almacenado en disco únicamente para almacenar información que tenga que ver con su labor, quedando rotunda y expresamente prohibido el uso de esta área para información de carácter personal. Esta unidad tendrá los mecanismos de respaldo que garanticen su total recuperación por parte de personal de la Subgerencia IT cuando el usuario propietario de la información lo requiera.

ADMINISTRACION: El administrador debe crear áreas para los usuarios donde se tengan definidas las jerarquías que fija esta política (anexo 10).

REVISION: En caso de reportarse pérdida o adulteración de información sobre áreas privadas, el administrador deberá presentar los archivos de seguimiento para determinar responsables de eliminación o modificación y seguirá la investigación requerida para hacer detección de intrusos.

PENALIZACION: De acuerdo con el nivel de daño y responsabilidad causado se aplicarán las sanciones que apliquen.

XVIII

POLITICA: El uso de servicios de mensajería instantánea a través de internet como msn messenger, chat, icq estará autorizado solamente para aquellos usuarios que mediante comunicación escrita del jefe inmediato justifiquen su uso,

el cual será para efectos de comunicación con entes externos que tengan que ver con la labor propia del funcionario solicitante.

ADMINISTRACION: Se definen las políticas de seguridad que garanticen el uso de estos recursos de acuerdo con la política actual.

REVISION: En caso de detectarse el uso no autorizado de productos de mensajería se verificará el porqué técnicamente es posible, se buscarán y aplicarán los correctivos del caso para prevenir que este tipo de situación se vuelva a presentar y se informará al usuario sobre esta falla, en caso de reincidencia se enviará comunicación a recursos humanos.

PENALIZACION: Primer aviso, comunicación a recursos humanos, demás que procedan.

XIX

POLITICA: Los servicios de terminal virtual y transferencia de archivos a los servidores Solaris de bases de datos se hará mediante protocolos seguros que manejen encripción y claves de seguridad, su acceso se autorizará solamente al personal técnico que lo requiera.

ADMINISTRACION: El administrador de los servidores instalará los servicios seguros ssh y sftp y cerrará de manera permanente los puertos telnet y ftp.

REVISION: Se harán pruebas esporádicas de la imposibilidad de conexión através de telnet y ftp.

PENALIZACION: Debido a que la responsabilidad es de carácter exclusivo del administrador y operador de la plataforma se hará un llamado de atención por parte del Subgerente en caso de incumplimiento, en caso de reincidencia se hará el llamado de atención con copia a la hoja de vida y demás que procedan

XX

POLITICA: Se definirán niveles jerárquicos para los usuarios unix a fin de controlar su uso y gestión.

ADMINISTRACION: Se definen las siguientes jerarquías y manejo:

Usuario privilegiado: Los usuarios de alto nivel como root, oracle, etc, tendrán cambio de contraseña cada 3 meses y sus claves serán solamente conocidas por el administrado y operador, adicionalmente se entregan en sobre sellado al Subgerente de Informática y Tecnología, dicho sobre solamente será abierto en

caso de contingencia severa y en ausencia del administrador y/o operador, siendo responsabilidad del Subgerente de IT a quien entrega las claves.

Usuario de trabajo: Los usuarios de trabajo de las aplicaciones que lo requiere (sintel, sigar), tendrán cambio de contraseña cada 3 meses y sus claves serán conocidas por los administradores de la aplicación, estos usuarios tienen acceso a través de terminales virtuales por lo cual NO DEBEN pertenecer a los grupos: dba, root o sysadm, a fin de evitar daño por sabotaje o error involuntario.

Usuario de conexión simple: Estos usuarios son los que se utilizan para realizar conexiones virtuales fijas (DAD Database access descriptor) o variables (samba), estos usuarios no tienen posibilidad de abrir terminales virtuales y NO DEBEN pertener a ninguno de los grupos: dba, root o sysadm.

REVISION: Se harán pruebas esporádicas del cumplimiento de esta política y teniendo en cuenta que la creación de usuarios unix es muy poco frecuente se aplicará cuando se cree un nuevo usuario.

PENALIZACION: Debido a que la responsabilidad es de carácter exclusivo del administrador y operador de la plataforma se hará un llamado de atención por parte del Subgerente en caso de incumplimiento, en caso de reincidencia se hará el llamado de atención con copia a la hoja de vida y demás que procedan

XXI

POLITICA: La definición y acceso a carpetas compartidas se hará mediante solicitud escrita o electrónica de cualquiera de los Directivos, para el caso de las semipúblicas, la información aquí almacenada es considerada importante por lo cual se incluirá en el backup diferencial y completo del servidor de red, adicionalmente se definirá una carpeta de intercambio con acceso completo para todos los usuarios de la red corporativa, denominada k:\publico, la información almacenada en esta carpeta es considerada temporal y solamente se hará backup de la misma en el backup completo del servidor de red.

ADMINISTRACION: Una vez se recibe la solicitud del Directivo o se detecta la necesidad de almacenamiento compartido se creará la carpeta, por defecto se crea con 20 megas pero en caso de justificarse la necesidad se ampliará la capacidad hasta 200megas.

REVISION: No se requiere.

PENALIZACION: No aplica.

XXI

POLITICA: Los usuarios pueden decidir si usar o no protector de pantalla en sus equipos.

ADMINISTRACION: Se hará una campaña a fin de informar a los usuarios la importancia de usar el protector de pantalla a fin de evitar el acceso a información por parte de personal no autorizado en ausencia del usuario, sin embargo su uso no será obligatorio.

REVISION: No se requiere.

PENALIZACION: No aplica.

XXII

POLITICA: Queda expresamente prohibido el almacenamiento de archivos considerados entretenimiento como música, video, fotografías, animaciones cuyo contenido no corresponda a fines laborales.

ADMINISTRACION: Se hará una revisión cada seis meses de la información almacenada en los discos duros de los usuarios a fin de detectar contenido no autorizado.

REVISION: Con la revisión semestral, se rendirá informe al usuario y se eliminarán los archivos encontrados.

PENALIZACION: Cuando se encuentren archivos prohibidos por primera vez se hará la advertencia al usuario directamente, en caso de reincidencia se informará al Jefe Inmediato, si la situación se vuelve a presentar con el mismo usuario sin importar que sea en otro equipo se informará a recursos humanos para aplicar los recursos que procedan.

XXIII

POLITICA: Para los equipos de cómputo (microcomputadores y portátiles) que posean puertos usb, y acceso a estos equipo a través de infrarrojos, bluetoooth y demás elementos deberán ser utilizados únicamente para propósitos legítimos del negocio. Se permite que los usuarios los utilicen para facilitarles el desempeño de sus tareas.

ADMINISTRACION: El uso de estos elementos y/o dispositivos son un privilegio que puede ser revocado en cualquier momento y el uso incorrecto de los mismos será responsabilidad única y exclusivamente del responsable del equipo sobre el cual se utilicen los mismos.

REVISION: En caso de recibir reporte del manejo inadecuado de estos elementos o dispositivos, se hará un llamado de atención por el incumplimiento de esta política y aplicar las penalizaciones.

PENALIZACION: Si se comprueba el uso indebido del correo se hará un llamado de atención, en caso de reincidencia se suspenderá el acceso a dichos puertos y por una tercera falla se retirará de manera definitiva con comunicación a la Dirección de Recursos Humanos para que aplique las sanciones que apliquen

XXIV

POLITICA: Aprovechando la facilidad de montaje de conexiones de alta velocidad DSL con la red corporativa, usuarios con funciones críticas dentro de la organización podrán tener configurados enlaces de datos para permitir el "Teletrabajo"; dicha facilidad permitirá atender oportunamente, situaciones que requieran de su inmediata participación permitiendo con ello el flujo de los procesos.

ADMINISTRACION: Se mantendrá debidamente actualizada, la relación de las personas que cuentan con enlaces de datos, incluyendo fechas de instalación, dispositivos entregados, ancho de banda, linea telefónica usada para la comunicación y nombre de la persona que efectuó la instalación. El uso de estas conexiones, elementos y/o dispositivos son un privilegio que puede ser revocado en cualquier momento y el uso incorrecto de los mismos será responsabilidad única y exclusivamente de la persona que tiene instalado el enlace de comunicaciones.

REVISION: En caso de recibir reporte del manejo inadecuado de estas conexiones, se hará un llamado de atención por el incumplimiento de esta política y se aplicarán las penalizaciones.

PENALIZACION: Si se comprueba el uso indebido de la conexión remota establecida con la red empresarial, se hará un llamado de atención y en caso de reincidencia se inhabilitará el enlace de datos y por una tercera falla se retirará de manera definitiva con comunicación a la Dirección de Recursos Humanos para que aplique las sanciones del caso.

XXV

POLITICA: Los usuarios de producción tendrán un vencimiento de 90 días, con un tiempo de no reuso de un año y se exigirá que la contraseña tenga como mínimo 10 caracteres, debe contener letras y números, debe diferir por lo menos en tres caracteres de la clave anterior.

ADMINISTRACION: Todo nuevo usuario propietario de objetos será creado con el profile de administración.

REVISION: Anualmente se hará una verificación de usuarios creados y sus profiles.

PENALIZACION: Si se encuentran usuarios con profiles que no coinciden o sin profile se verificará quien creó el usuario para hacer el respectivo recorderis de esta política.

HE LEIDO, ENTIENDO Y ACEPTO LAS POLITICAS DE SEGURIDAD INFORMATICA DE TELEBUCARAMANGA

NOMBRE: _____

FECHA: _____

FIRMA: _____

ANEXO B: Matriz de riesgos Telebucaramanga.

INSTRUCCIONES PARA DILIGENCIAR LA MATRIZ DE RIESGOS El objetivo de la Matriz de Riesgos es identificar, analizar, evaluar y monitorear los riesgos que están afectando o pudieran afectar el logro de los objetivos del proceso que usted tiene a su cargo, con el fin de minimizar las pérdidas y maximizar las oportunidades. Por favor lea las siguientes instrucciones y diligencie junto con el personal que considere pertinente la Matriz de Riesgos de su proceso.

1. IDENTIFICACIÓN DEL RIESGO	
Consiste en determinar lo que puede suceder, por qué (causas) y las consecuencias. Empiece diligenciando la Hoja "Identificación" las columnas B, C y D, según las siguientes indicaciones.	
Columna B:Qué puede suceder	Liste todos los eventos internos y externos que podrían ocurrir en cada una de las actividades que conforman su proceso y que impedirían alcanzar el objetivo, utilice como guía las actividades listadas en la Caracterización del proceso.
Columna C:Cómo y porqué?	Describa todas las causas y formas en las que se puede iniciar el evento, tenga presente las causas originadas por las 5M: máquina, mano de obra, materiales, método y medio ambiente.
Columnna D. Redacción del riesgo	Redacte cada riesgo de la siguiente manera: "qué puede suceder" + "debido a que" + "causa"

2. ANÁLISIS DEL RIESGO	
El objetivo del análisis de riesgos consiste en separar los riesgos menores de los mayores y proporcionar datos que sirvan para la evaluación y tratamiento del riesgo. Para esto identifique los controles sobre los riesgos identificados, y permita que cada uno de los miembros del grupo asigne calificaciones individuales de probabilidad e impacto. La hoja de calculo consolidará la información de todos los participantes y se obtendrá el Nivel del Riesgo.	
Columna C: Controles existentes	Liste todos los controles: procedimientos, sistemas técnicos, políticas, etc. que existen actualmente para controlar el riesgo.Tenga en cuenta la información consignada en la Caracterización del proceso asociada con Parámetros de control.
Columna D: Probabilidad	Asigne **1**, si la probabilidad de que este riesgo ocurra realmente es **ocasional o baja en un año.** **2**, si la probabilidad pueda presentarse **algunas veces en un año.** **3**, si es probable que ocurra **muchas veces en un año.**
Columna E: Impacto	Asigne **5**, si el impacto no afecta de manera significativa y puede ser asumido por el giro normal de las operaciones del prestador ya que no afecta la operación del servicio, la viabilidad empresarial o la relación con el usuario, los efectos (operativos, financieros, de imagen, etc) sobre la empresa al ocurrir este evento son **menores**. **10,** se puede ver afectada la eficiencia del prestador disminuyéndose la calidad del servicio, generando insatisfacción en el usuario y retrasos en la operación, en este caso los efectos son **importantes** **20,** si los efectos son **mayores** cuando se afectan los estándares de los indicadores, se generan incumplimientos regulatorios, se puede poner en riesgo la prestación del servicio, la viabilidad

	empresarial y se afecta la relación con el usuario.
Columna AF: Nivel del Riesgo Absoluto	Resulta de multiplicar la calificación de la probabilidad por el impacto de su consecuencia, su objetivo es permitir evaluar el riesgo para establecer prioridades.
3. EVALUACIÓN DEL RIESGO La evaluación del riesgo consiste en determinar las prioridades de gestión de riesgos mediante la comparación del Nivel del Riesgo contra estándares determinados.* * Telebucaramanga adoptó los estándares propuestos por el DAFP en la Guía de Administración de Riesgo	
Columna AG: Evaluación del Riesgo	La hoja de cálculo automáticamente clasificará los riesgos en Inaceptable, Importante, Moderado, Tolerable, o Aceptable de acuerdo a los siguientes Niveles de Riesgo. INACEPTABLE: Nivel de Riesgo= 60. IMPORTANTE: Nivel de Riesgo= 30 o 40. MODERADO: Nivel de Riesgo=15 0 20. TOLERABLE: Nivel de Riesgo=10 ACETABLE: Nivel de Riesgo=5. Usted debe ubicar los riesgos en la Gráfica de Riesgos. Este paso tiene como fin visualizar los diferentes tipos de riesgos para tomar las medidas que se consideren pertinentes.
4. TRATAMIENTO DE RIESGOS	

Pase a la hoja de cálculo: Tratamiento de Riesgos y diligencie el plan de acción para los riesgos que lo requieran de acuerdo a la siguienter descripción:*

INACEPTABLE: Es aconsejable eliminar la actividad que genera el riesgo en la medida que sea posible, de lo contrario se deben implementar controles para evitar la probabilidad, disminuir el impacto o compartir o transferir el riesgo si es posible a través de pólizas de seguros u otras opciones que estén disponibles. (evitar, reducir , compartir)

IMPORTANTE: Se deben tomar medidas para bajar el valor del riesgo, si es posible fortalecer y mejorar controles existentes(red evitar, compartir)

MODERADO: Se pueden tomar medidas para bajar el valor del riesgo, si es posible, se deben conservar y mejorar controles (reducir, compartir)

TOLERABLE: Se puede realizar un análisis del costo beneficio con el que se pueda decidir entre reducir el riesgo, asumirlo o compartirlo.

ACETABLE: Se acepta el riesgo sin necesidad de tomar otras medidas de control diferentes a las que se poseen.

* Fuente: DAFP Guía de Administración del Riesgo, adaptada a Telebucaramanga.

Código: P01.GRI.F01
Versión:4

GESTIÓN DE RIESGOS
IDENTIFICACIÓN DE RIESGOS POR PROCESO

PROCESO: Informática y Tecnología

FECHA DE REVISIÓN: 27-03-2008

REF	1. IDENTIFICACIÓN DEL RIESGO		
	Objetivo del Proceso: Desarrollar y suministrar servicios de soluciones informáticas y telemáticas de manera ágil, eficiente y oportuna, aplicando el conocimiento y profesionalismo de nuestra gente e incorporando los últimos avances tecnológicos en materia de software, hardware y comunicaciones, que le permitan a la empresa contar con información clara y veraz para la toma de decisiones de forma táctica y estratégica.		
	¿Qué puede suceder?	¿Cómo? ¿Por qué? (causa)	Descripción del Riesgo
1	Pérdida de uno, varios o todos los archivos log	Eliminación por error humano Daño en disco	Pérdida de uno, varios o todos los archivos log debido a eliminación por error humano o daño en disco
2	No contar con archivos log que permitan detectar las posibles fallas de las bases de datos o acciones sobre ellas (insert, delete, update).	No esté parametrizado	No contar con archivos log que permitan detectar las posibles fallas de las bases de datos o acciones sobre ellas (insert, delete, update), debido a que no están parametrizados.
3	Que no existan backups	Incumplimiento del cronograma de backups	Inexistencia de backups debido al incumplimiento del cronograma de backups
4	Pérdida de un datafile	Eliminación por error humano Daño en disco No esté registrado en el filesystem	Pérdida de un datafile, debido a eliminación por error humano, daño en disco o no esté registrado en el filesystem
5	Pérdida de uno, varios o todos los archivos de root	Eliminación por error humano Daño en disco	Pérdida de uno, varios o todos los archivos de root debido a eliminación por error humano o daño en disco
6	Pérdida de uno, varios o todos los archivos de los file systems de trabajo (/tollt, /srh, /facturas, etc)	Eliminación por error humano Daño en disco	Pérdida de uno, varios o todos los archivos de los file systems de trabajo (/tollt, /srh, /facturas, etc), debido a eliminación por error humano o daño en disco.

7	Daño de una parte hardware (tarjeta de red, fuente de poder, disco ,etc) en los servidores de bases de datos y de red	Falta de realización de los mantenimientos preventivos Falla o caída eléctrica Condiciones ambientales inadecuadas Sabotaje Catástrofe natural	Daño de una parte hardware (tarjeta de red, fuente de poder, disco ,etc) en los servidores de bases de datos y de red, debido a falta de realización de los mantenimientos preventivos, falla o caída eléctrica, condiciones ambientales inadecuadas, sabotaje o catástrofe natural.
8	Fallo total hardware -daño en el servidor bases de datos y/o en el servidor de red	Falta de realización de los mantenimientos preventivos Falla o caída eléctrica Condiciones ambientales inadecuadas Sabotaje Catástrofe natural	Fallo total hardware -daño en el servidor bases de datos y en el servidor de red, debido a falta de realización de los mantenimientos preventivos, falla o caída eléctrica, condiciones ambientales inadecuadas, sabotaje o catástrofe natural.
9	Daño de un elemento activo de red - no core	Falta de realización de los mantenimientos preventivos Falla o caída eléctrica Condiciones ambientales inadecuadas Sabotaje Catástrofe natural Falta de seguridad en los cuartos de comunicaciones	Daño de un elemento activo de red - no core, debido a falta de realización de los mantenimientos preventivos, falla o caída eléctrica,condiciones ambientales inadecuadas, sabotaje, catástrofe natural, falta de seguridad en los cuartos de comunicaciones.
10	Daño de un elemento activo de red- core	Falta de realización de los mantenimientos preventivos Falla o caída eléctrica Condiciones ambientales inadecuadas Sabotaje Catástrofe natural Falta de seguridad en los cuartos de comunicaciones	Daño de un elemento activo de red - core, debido a falta de realización de los mantenimientos preventivos, falla o caída eléctrica,condiciones ambientales inadecuadas, sabotaje, catástrofe natural o falta de seguridad en los cuartos de comunicaciones.
11	Imposibilidad de acceso a la sede principal	Sabotaje Catástrofe	Imposibilidad de acceso a la sede principal debido a sabotaje o catástrofe.

12	Daño de un disco duro en el servidor X-Mate - Interno	Falta de realización de los mantenimientos preventivos Falla o caida eléctrica No contar con las condiciones ambientales adecuadas Sabotaje Catástrofe natural	Daño de un disco duro en el servidor X-Mate - Interno, debido a falta de realización de los mantenimientos preventivos, falla o caida eléctrica, no contar con las condiciones ambientales adecuadas, sabotaje o catástrofe natural.
13	Daño de un disco duro en el multipack externo de Xmate	Falta de realización de los mantenimientos preventivos Falla o caida eléctrica No contar con las condiciones ambientales adecuadas Sabotaje Catástrofe natural	Daño de un disco duro en el servidor X-Mate - Externo, debido a falta de realización de los mantenimientos preventivos, falla o caida eléctrica, no contar con las condiciones ambientales adecuadas, sabotaje o catástrofe natural.
14	Obtención de resultados inesperados en el desarrollo de software	No contar con un plan exhaustivo de pruebas de software	Obtención de resultados inesperados en el desarrollo de software debido a la falta de implementación de un plan exhastivo de software
15	Software desarrollado que no satisface la necesidad del cliente	Mala interpretación de los requerimientos de desarrollo Que no existan estándares de programación	Desarrollo de software que no satisface las necesidades, debido a mala interpretación de los requerimientos de desarrollo o por la inexistencia de estándares de programación.
16	Que la solución software no sea entregada en el tiempo programado inicialmente	Fallas en la planeación del desarrollo Dependencia del tiempo de los clientes Cambio de directrices gerenciales que afectan la planeación anual de las actividades de desarrollo de software No contar con el recurso humano suficiente para desarrollar el software	Incumplimiento en el tiempo estipulado para entregar el sotware, debido a fallas en la planeación del desarrollo, dependencia del tiempo de los clientes, cambio de directrices gerenciales que afectan la planeación anual de las actividades de desarrollo de software, o que no se cuente con el recurso humano suficiente para desarrollar el software
17	Mala utilización del software	Que no exista documentación del software desarrollado o adquirido Que no se dé la adecuada capacitación al cliente interno del sofware desarrollado	Mala utilización del software, debido a que no existe documentación del software desarrollado o adquirido, o que no se dé la adecuada capacitación al cliente interno del sofware desarrollado.

18	Imposibilidad de desarrollar e implementar sotware requerido	Desconocimiento del funcionamiento interno de plataformas tecnológicas cerradas (Ericsson, Unisys) Falta de presupuesto para la implementación o adquisición de una solución	Imposibilidad de desarrollar e implementar sotfware requerido debido a desconocimiento del funcionamiento interno de plataformas tecnológicas cerradas (Ericsson, Unisys), o falta de presupuesto para la implementación o adquisición de una solución
19	Mala asignación del perfil solicitado	Mal diligenciamiento de los formatos de solicitud de acceso Falta de control por parte del encargado de autorizar la asignación del perfíl.	Asignación incorrecta de perfil de usuario, debido a que se diligenció erroneamente el formato de solicitud de acceso o por falta de control por parte del encargado de autorizar la asignación del perfíl.
20	Ejecución de procesos por personas no autorizadas	Mal uso de las cuentas asignadas Falta de información de las novedades de personal (traslados, retiros, etc.) para mantener actualizadas las cuentas de usuarios	Ejecución de procesos por personas no autorizadas, debido al mal uso de las cuentas asignadas por la falta de información sobre novedades de personal (traslados, retiros, etc).
21	Eliminación errada de cuentas de usuario activos y de procesos críticos	Error humano	Eliminación errada de cuentas de usuario activos y de procesos críticos, debido a error humano.
22	Caida de la página web de la Empresa	No realizar mantenimientos preventivos al servidor web Falla o caida eléctrica No contar con las condiciones ambientales adecuadas Sabotaje Catástrofe natural Instalación inadecuada del software	Caida en la página de web de la Empresa, por no realizar mantenimientos preventivos, por falla o caida eléctrica, por no contar con las condiciones ambientales adecuadas, sabotaje, catástrofe natural, instalación inadecuada del software.
23	Desactualización de la información publicada en la intranet	Incumplimiento de políticas	Desactualización de la información en la intranet, debido al incumplimiento de políticas.
24	Desactualización de la información publicada en la pagina web de la Empresa	Falta de cumplimiento de politicas y procedimientos	Desactualización de información en la página web de la Empresa, debido al incumplimiento de políticas y de procedimientos.
25	No identificación en la red de los puntos de voz y datos.	No contar con un plano actualizado de la red de voz y datos	No identificar los puntos de voz y datos, debido a la desactualización del plano

26	Pasar a producción una versión anterior de un objeto crítico.	Error humano	Pasar a producción una versión anterior de un objeto crítico debido a error humano
27	Ataques informáticos a través del servicio de internet corporativo o correo electrónico	No tener la versión antivirus actualizada. No contar con software especializado (Firewalls).	Ataques informáticos a través de internet o correo electrónico, por no tener la versión antivirus actualizada o por no contar con software especializado (firewalls)

MATRIZ PARA ANALIZAR Y EVALUAR RIESGOS

Código: P01.GRI.F01

Proceso: Informática y Tecnología

Versión: 4

Fecha Revisión: MARZO 25 de 2008

REF	1. DESCRIPCIÓN DEL RIESGO	2. ANÁLISIS DEL RIESGO	3.

		Controles existentes	P1		P2		P3		PROBABILIDAD	IMPACTO	NIVEL DE RIESGO	EVALUACIÓN DEL RIESGO
			P	I	P	I	P	I				
20	Ejecución de procesos por personas no autorizadas, debido al mal uso de las cuentas asignadas por la falta de información sobre novedades de personal (traslados, retiros, etc).	Se tiene definido el proceso para el reporte de novedades por parte de Gestión Humana para realizar el mantenimiento sobre las cuentas de acceso y se hace seguimiento al cumplimiento, adicionalmente el servidor de base de datos elimina las cuentas inactivas de manera automática, se diligencia el campo fecha de expiración en las cuentas de red para todos los contratistas y temporales para realizar automáticamente la inactivación de este tipo de usuarios	2	10	2	10	2	10	2	10	20	MODERADO
8	Fallo total hardware -daño en el servidor bases de datos y en el servidor de red, debido a falta de realización de los mantenimientos preventivos, falla o caída eléctrica, condiciones ambientales inadecuadas, sabotaje o catástrofe natural.	**Daño en servidor de base de datos:** Configuración de base de datos en modo standby. Sistemas de detección - extinción de incendios, control de acceso en el centro de procesamiento. Máquina standby en un sitio seguro y distante de la máquina principal **Daño en servidor de red:** Se cuenta con un servidor cold backup. Se realiza semanalmente una copia de los objetos software de las aplicaciones a un pc para posibilitar su recuperación en caso de daño total hardware	1	20	1	20	1	20	1	20	20	MODERADO
25	No identificar los puntos de voz y datos, debido a la desactualización del plano	Se viene realizando el inventario de la red se ha completado en un 60%	3	5	3	5	3	5	3	5	15	MODERADO
5	Pérdida de uno, varios o todos los archivos de root debido a eliminación por error humano o daño en disco	Esta información se encuentra en los discos internos y se tiene configurado mirror total automático el cual en caso de falla del disco principal entra en funcionamiento sin intervención del operador. En caso de error humano se cuenta con backup completo de root en cinta	1	10	1	10	1	10	1	10	10	TOLERABLE

16	Incumplimiento en el tiempo estipulado para entregar el sotware, debido a fallas en la planeación del desarrollo, dependencia del tiempo de los clientes, cambio de directrices gerenciales que afectan la planeación anual de las actividades de desarrollo de software, o que no se cuente con el recurso humano suficiente para desarrollar el software	Se cuenta con una aplicación de software llamada “Bolsa de Solicitudes” que permite organizar el tiempo y los trabajos que adelanta cada integrante del equipo de desarrollo. Debido a la gran cantidad de imprevistos (muchas veces originados por fuerza mayor), se ha optado por no comprometer fechas de entrega, sino por manejar tiempos de desarrollo de cada actividad.	2	5	2	5	2	5	2	5	10	TOLERABLE

24	Desactualización de información en la página web de la Empresa, debido al incumplimiento de políticas y de procedimientos.	Se ha definido el procedimiento de reporte	2	5	2	5	1	5	2	5	10	TOLERABLE
3	Inexistencia de backups debido al incumplimiento del cronograma de backups	Los export son automáticos y los on-line son monitoreados semanalmente	1	10	1	10	1	10	1	10	10	TOLERABLE
7	Daño de una parte hardware (tarjeta de red, fuente de poder, disco ,etc) en los servidores de bases de datos y de red, debido a falta de realización de los mantenimientos preventivos, falla o caída eléctrica, condiciones ambientales inadecuadas, sabotaje o catástrofe natural.	**Daño de una parte hardware (tarjeta de red, fuente de poder, etc) servidor base de datos:** Contrato de mantenimiento preventivo y correctivo con SUN Microsystems que garantiza suministro de repuestos en 24 horas máximo. El servidor tiene fuentes de poder y tarjetas de red redundantes. **Daño de un disco servidor base de datos:** Los discos internos donde está root y el motor de base de datos se encuentran en mirror y el storage tiene dos discos en hot spare. Base de datos con servicio dataguard. **Daño de un disco servidor de red:** Se cuenta con un servidor de respaldo para reemplazo de partes **Daño de una parte hardware (tarjeta de red, fuentes de poder, etc) servidor de red:** Se cuenta con un servidor en cold standby para reemplazo de partes Los servidores tiene fuente de poder redundante	1	10	1	10	1	10	1	10	10	TOLERABLE

18	Imposibilidad de desarrollar e implementar sotfware requerido debido a desconocimiento del funcionamiento interno de plataformas tecnológicas cerradas (Ericsson, Unisys), o falta de presupuesto para la implementación o adquisición de una solución	Si la plataforma tecnológica a modificar es desconocida, esta situación se hace conocer con anticipación a la formulación de cronogramas o planes de implementación, con el fin de que la Empresa pueda inciar la busqueda de los consultores, técnicos o asesores que de manera conjunta con personal interno ejecuten las actividades pertinentes.	1	10	1	10	1	10	1	10	10	TOLERABLE

11	Imposibilidad de acceso a la sede principal debido a sabotaje o catástrofe.	En caso de no poder accesar a las sedes de la Empresa, se haría el acceso desde los sitios remotos: Punto Cañaveral, Call Center, en caso de no tener comunicación remota por daños en la fibra óptica las labores se realizarán desde el call center que tiene conexión directa, se cuenta con un sitio alterno donde están replicadas las bases de datos, en la sede principal no se encuentra ningún servidor, las copias de seguridad se encuentran almacenadas en sitio alterno y bóveda de seguridad	1	5	1	5	1	5	1	5	5	ACEPTABLE
26	Pasar a producción una versión anterior de un objeto crítico debido a error humano	El paso de objetos a producción se encuentra automatizado y se reforzará con un proceso de control de calidad por parte del área de software, adicionalmente se disminuye el impacto ya que se cuenta con backup diario de los fuentes tanto a nivel de scripts como de objetos cliente (formas, reportes, menú)	1	5	1	5	1	5	1	5	5	ACEPTABLE
4	Pérdida de un datafile, debido a eliminación por error humano, daño en disco o no esté registrado en el filesystem	Se tienen las instancias de producción configuradas en dataguard, lo que garantiza copia en disco online en máquina separada de todos los datafiles. El arreglo de discos tiene discos en hotspare que entran en funcionamiento en caso de daño hardware de un disco. Todos los datafiles están respaldados por las copias de seguridad. La base de datos está configurada en modo archive log, Los storage array tienen discos en hot spare para recuperación en caso de daño, Se realiza backup semanal y todas las instancias están en modo archive-log	1	5	1	5	1	5	1	5	5	ACEPTABLE
6	Pérdida de uno, varios o todos los archivos de los file systems de trabajo (/tollt, /srh, /facturas, etc), debido a eliminación por error humano o daño en disco.	Se tienen los storage configurados con discos en hotspare. Se toma backup diario de los file systems de movimiento, En caso de error humano se cuenta con backup completo diario de los filesystems de movimiento	1	5	1	5	1	5	1	5	5	ACEPTABLE
10	Daño de un elemento activo de red - core, debido a falta de realización de los mantenimientos preventivos, falla o caída eléctrica,condiciones ambientales inadecuadas, sabotaje, catástrofe natural o falta de seguridad en los cuartos de comunicaciones.	Se cuenta con un switch de respaldo que soporta la carga de todos los elementos de red, por el momento funciona como respaldo en frio pero se realizará el tendido para contar con contingencia on-line utilizando los elementos existentes.	1	5	1	5	1	5	1	5	5	ACEPTABLE
14	Obtención de resultados inesperados en el desarrollo de software debido a la falta de implementación de un plan exhastivo de software	El personal de desarrollo cuenta con un ambiente de pruebas que le permite ejecutar sobre ellas simulaciones de comportamiento del software implementado en condiciones similares al ambiente de producción.	1	5	1	5	1	5	1	5	5	ACEPTABLE

19	Asignación incorrecta de perfil de usuario, debido a que se diligenció erroneamente el formato de solicitud de acceso o por falta de control por parte del encargado de autorizar la asignación del perfíl.	El formato de solicitud de acceso aprobado por el jefe inmediato, se realiza anualmente la revisión de perfiles con los responsables de área	1	5	1	5	1	5	1	5	5	ACEPTABLE
27	Ataques informáticos a través de internet o correo electrónico, por no tener la versión antivirus actualizada o por no contar con software especializado (firewalls)	Se dispone de un software antivirus y se actualiza de manera periódica (3 veces a la semana) Se cuenta con un elemento perimetral de seguridad que controla el tráfico desde y hacia internet con módulos antispyware, antivirus, firewall, detección de intrusos y filtrado de contenido	1	5	1	5	1	5	1	5	5	ACEPTABLE

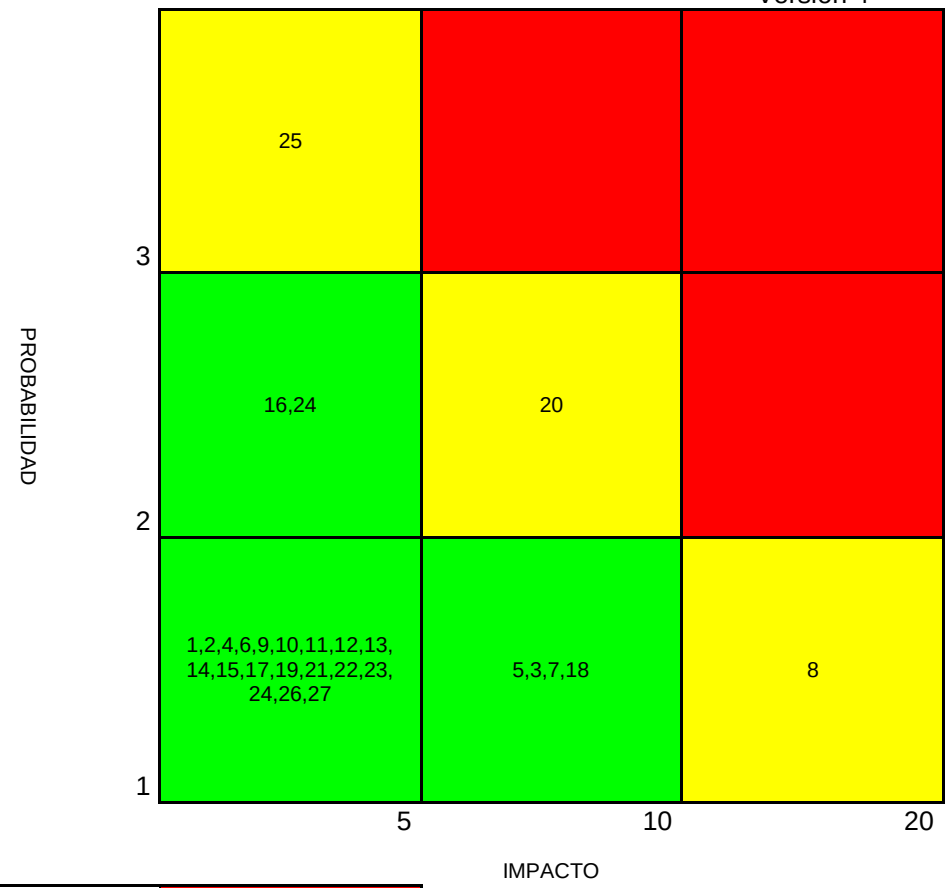
1	Pérdida de uno, varios o todos los archivos log debido a eliminación por error humano o daño en disco	Se toman dos copias de los log. Se tienen todas las instancias configuradas en dataguard, lo que garantiza copia en disco online en máquina separada de los logs generados. El arreglo de discos tiene discos en horspare que entran en funcionamiento en caso de daño hardware de un disco.	1	5	1	5	1	5	1	5	5	ACEPTABLE
2	No contar con archivos log que permitan detectar las posibles fallas de las bases de datos o acciones sobre ellas (insert, delete, update), debido a que no están parametrizados.	Se verifica que todos los Logs de la base de datos se encuentren respaldados con copias de seguridad adicionalmente se cuenta con export diario de todas las instancias para efectos de recuperación de información en el tiempo, adicionalmente se encuentra activada la opción de auditoría sobre la base de datos	1	5	1	5	1	5	1	5	5	ACEPTABLE
9	Daño de un elemento activo de red - no core, debido a falta de realización de los mantenimientos preventivos, falla o caída eléctrica,condiciones ambientales inadecuadas, sabotaje, catástrofe natural, falta de seguridad en los cuartos de comunicaciones.	Se tienen elementos y conectores en stock para atender este tipo de falla	1	5	1	5	1	5	1	5	5	ACEPTABLE

12	Daño de un disco duro en el servidor X-Mate - Interno, debido a falta de realización de los mantenimientos preventivos, falla o caida eléctrica, no contar con las condiciones ambientales adecuadas, sabotaje o catástrofe natural.	Se cuenta con otra máquina de iguales características para respaldo. Se cuenta con backups diarios de este servidor Contrato de mantenimiento preventivo	1	5	1	5	1	5	1	5	5	ACEPTABLE

15	Desarrollo de software que no satisface las necesidades, debido a mala interpretación de los requerimientos de desarrollo o por la inexistencia de estándares de programación.	Es labor de los analistas, acordar con claridad los requerimientos por parte de los usuarios finales en las fases previas al desarrollo. Antes de poner en producción los cambios implementados, se ejecutan controles de calidad que minimicen este riesgo. El usuario final se involucra cuando se requiera, en la labor de desarrollo analizando resultados parciales.	1	5	1	5	1	5	1	5	5	ACEPTABLE
22	Caida en la página de web de la Empresa, por no realizar mantenimientos preventivos, por falla o caida eléctrica, por no contar con las condiciones ambientales adecuadas, sabotaje, catástrofe natural, instalación inadecuada del software.	Se cuenta con backup en el equipo del web master de fuentes y ejecutables de la página web, se tiene configurado el servidor web en otro de los servidores corporativos	1	5	1	5	1	5	1	5	5	ACEPTABLE
23	Desactualización de la información en la intranet, debido al incumplimiento de políticas.	Se ha definido el procedimiento de reporte	1	5	1	5	1	5	1	5	5	ACEPTABLE
13	Daño de un disco duro en el servidor X-Mate - Externo, debido a falta de realización de los mantenimientos preventivos, falla o caida eléctrica, no contar con las condiciones ambientales adecuadas, sabotaje o catástrofe natural.	Se cuenta con otra máquina de iguales características para respaldo. Se cuenta con backups diarios de este servidor Contrato de mantenimiento preventivo	1	5	1	5	1	5	1	5	5	ACEPTABLE
17	Mala utilización del software, debido a que no existe documentación del software desarrollado o adquirido, o que no se dé la adecuada capacitación al cliente interno del sofware desarrollado.	Cuando el desarrollo lo amerite, se adelantan jornadas de capacitación con los usuarios lideres; de acuerdo con la metodologia de desarrollo que se tiene, se involucra al usuario en las pruebas al software que se modifica o desarrolla.	1	5	1	5	1	5	1	5	5	ACEPTABLE
21	Eliminación errada de cuentas de usuario activos y de procesos críticos, debido a error humano.	Si bien la eliminación del usuario y sus recursos de red es posible, se cuenta con backup diario para efectos de recuperación	1	5	1	5	1	5	1	5	5	ACEPTABLE

PROCESO: **Informática y Tecnología**

Versión 4



INACEPTABLE	
IMPORTANTE	
MODERADO	
TOLERABLE	
ACEPTABLE	

GESTIÓN DE RIESGOS
PLAN DE ACCIÓN PARA EL TRATAMIENTO DE RIESGOS

PROCESO Informática y Tecnología **FECHA ELABORACIÓN PLAN** **E**

DESCRIPCIÓN DEL RIESGO	EVALUACIÓN DEL RIESGO	ACTIVIDAD	RECURSOS	RESPONSABLE	FECHA PROGRAM
Ejecución de procesos por personas no autorizadas, debido al mal uso de las cuentas asignadas por la falta de información sobre novedades de personal (traslados, retiros, etc).	MODERADO	Comunicación a Gestión Humana para recibir el reporte diario de novedades, adicionalmente a diario se ejecuta el proceso de verificación de fechas de conexión al servicor de red y las cuentas de la base de datos son monitoreadas de manera automática todos los días.		Néstor Javier Salazar	Permanente
Fallo total hardware -daño en el servidor bases de datos y en el servidor de red, debido a falta de realización de los mantenimientos preventivos, falla o caída eléctrica, condiciones ambientales inadecuadas, sabotaje o catástrofe natural.	MODERADO	El servidor de base de datos está en dataguard, para replicación automática se tiene un esquema de back up para los dos servidores y almacenamiento en bóvedad de seguridad para los back ups.		Néstor Javier Salazar	Permanente
No identificar los puntos de voz y datos, debido a la desactualización del plano	MODERADO	Adelantar el inventario completo de la red	Practicante	Carlos Ernesto Parra	30 de Abril 20
Pérdida de uno, varios o todos los archivos de root debido a eliminación por error humano o daño en disco	TOLERABLE	Se tiene un disco en hot spare en los arreglos y back up mensual.		Néstor Javier Salazar	Permanente

Incumplimiento en el tiempo estipulado para entregar el sotware, debido a fallas en la planeación del desarrollo, dependencia del tiempo de los clientes, cambio de directrices gerenciales que afectan la planeación anual de las actividades de desarrollo de software, o que no se cuente con el recurso humano suficiente para desarrollar el software	TOLERABLE	Se debe establecer las prioridades, pactando con los usuarios nuevas fechas teniendo en cuenta el perfil de las solicitudes requeridasque afectaron toda la programación inicial.		Humberto Rueda	Eventual
Desactualización de información en la página web de la Empresa, debido al incumplimiento de políticas y de procedimientos.	TOLERABLE	Diariamente se revisa esta información.		Carlos Ernesto Parra	Permanente
Inexistencia de backups debido al incumplimiento del cronograma de backups	TOLERABLE	Al inicio de semana se hace una revisión del diccionario de datos para verificar la ejecución del back up, por estar en la base de datos en modo archive-log se puede hacer recovery aún con back ups antíguos.		Néstor Javier Salazar	Permanente
Daño de una parte hardware (tarjeta de red, fuente de poder, disco ,etc) en los servidores de bases de datos y de red, debido a falta de realización de los mantenimientos preventivos, falla o caída eléctrica, condiciones ambientales inadecuadas, sabotaje o catástrofe natural.	TOLERABLE	Se cuenta con contrato de mantenimiento para reemplazo de partes y mano de obra en caso de daño.		Néstor Javier Salazar	Eventual
Imposibilidad de desarrollar e implementar sotfware requerido debido a desconocimiento del funcionamiento interno de plataformas tecnológicas cerradas (Ericsson, Unisys), o falta de presupuesto para la implementación o adquisición de una solución	TOLERABLE	Efectuar un análisis de las necesidades puntuales de área usuaria, para que con ello se estructuren RFI´s o RFP´s con las especificaciones requeridas.	Necesidades puntuales ya expresadas por el área usuaria.	Humberto Rueda	Eventual

Imposibilidad de acceso a la sede principal debido a sabotaje o catástrofe.	ACEPTABLE	La sala de sevidores y el servidor alterno se encuentran fuera de las instalaciones de Telebucaramanga en sedes privadas lo que minimiza el riesgo de sabotaje, en cuanto a catátrofe se cuenta con almacenamiento de copias de seguridad en bóvedas de seguridad.	Servidor de respaldo, contrato de almacenamiento de medios en bóveda de seguridad.	Néstor Javier Salazar	Eventual
Pasar a producción una versión anterior de un objeto crítico debido a error humano	ACEPTABLE	Si bien es posible que suceda, volver atrás es fácil y casi inmediato tanto en los objetos cliente como en los de la base de datos, este riesgo debería tener menor evaluación.		Néstor Javier Salazar	Eventual
Pérdida de un datafile, debido a eliminación por error humano, daño en disco o no esté registrado en el filesystem	ACEPTABLE	Se tiene un disco en hot spare en los arreglos, instancias configuradas en data guard y back up semanal.		Néstor Javier Salazar	Permanente
Pérdida de uno, varios o todos los archivos de los file systems de trabajo (/tollt, /srh, /facturas, etc), debido a eliminación por error humano o daño en disco.	ACEPTABLE	Se tiene un disco en hot spare en los arreglos y back up diario.		Néstor Javier Salazar	Permanente
Daño de un elemento activo de red - core, debido a falta de realización de los mantenimientos preventivos, falla o caída eléctrica,condiciones ambientales inadecuadas, sabotaje, catástrofe natural o falta de seguridad en los cuartos de comunicaciones.	ACEPTABLE	Se cuenta con un elemento de respaldo que soporta la carga completa del core.		Néstor Javier Salazar	Permanente

Obtención de resultados inesperados en el desarrollo de software debido a la falta de implementación de un plan exhastivo de software	ACEPTABLE	Se cuenta con un procedimeito formal de la compañía (P01.IYT) para llevar a cabo cualquier modificacion de software; en dicho procedimiento se involucran actividades de control de calidad y pruebas (efectuadas por personal distintoal programador original) y se debe contar con el Vo.Bo. del usuario final quién sobre el ambiente de desarrollo emite sus conceptos finales. No se pasa nada al ambiente de producción si no se cumplen con estos requisitos.	Personal de Crecimiento Informático	Humberto Rueda	Eventual
Asignación incorrecta de perfil de usuario, debido a que se diligenció erroneamente el formato de solicitud de acceso o por falta de control por parte del encargado de autorizar la asignación del perfíl.	ACEPTABLE	Semestralmente se realiza la revisión de perfiles de acceso a las aplicaciones.		Néstor Javier Salazar	Permanente
Ataques informáticos a través de internet o correo electrónico, por no tener la versión antivirus actualizada o por no contar con software especializado (firewalls)	ACEPTABLE	Se cuenta con un elemento perimetral de seguridad que tiene antivirus, antispyware, filtrado de contenido, firewall, detección de intrusos; se debe revisar la evaluación de este riesgo ya que se tiene cubierto.		Néstor Javier Salazar	Eventual
Pérdida de uno, varios o todos los archivos log debido a eliminación por error humano o daño en disco	ACEPTABLE	Se cuenta con dataguard en las instancias, disco en hotspare en los arreglos y en caso de presentarse basta con realizar un back up on-line completo.		Néstor Javier Salazar	Permanente

No contar con archivos log que permitan detectar las posibles fallas de las bases de datos o acciones sobre ellas (insert, delete, update), debido a que no están parametrizados.	ACEPTABLE	Se cuenta con log sobre las tablas críticas y se implementan cada vez que Auditoría lo solicita.		Néstor Javier Salazar	Eventual
Daño de un elemento activo de red - no core, debido a falta de realización de los mantenimientos preventivos, falla o caída eléctrica,condiciones ambientales inadecuadas, sabotaje, catástrofe natural, falta de seguridad en los cuartos de comunicaciones.	ACEPTABLE	Se tiene un elemento de contingencia para reemplazar cualquier elemento que tenga daño.		Néstor Javier Salazar	Eventual
Daño de un disco duro en el servidor X-Mate - Interno, debido a falta de realización de los mantenimientos preventivos, falla o caida eléctrica, no contar con las condiciones ambientales adecuadas, sabotaje o catástrofe natural.	ACEPTABLE	Los discos estan en mirror y se cuenta con un servidor adicional de back up en caso de daño.		Néstor Javier Salazar	Permanente
Desarrollo de software que no satisface las necesidades, debido a mala interpretación de los requerimientos de desarrollo o por la inexistencia de estándares de programación.	ACEPTABLE	Se cuenta con un procedimeito formal de la compañía (P01.IYT) para llevar a cabo cualquier modificacion de software; en dicho procedimiento se involucran actividades de control de calidad y pruebas (efectuadas por personal distintoal programador original) y se debe contar con el Vo.Bo. del usuario final quién sobre el ambiente de desarrollo emite sus conceptos finales. El usuario final emite sus comentarios sobre la interacción que persibe al momento de utilizar la herramienta modificada; en caso de que no se haya hecho un cambio que no corresponda con lo		Humberto Rueda	Permanente

		solicitado, el usuario no emite su OK y ello impide que los cambios sean llevados a producción.			
Caida en la página de web de la Empresa, por no realizar mantenimientos preventivos, por falla o caida eléctrica, por no contar con las condiciones ambientales adecuadas, sabotaje, catástrofe natural, instalación inadecuada del software.	ACEPTABLE	Se cuenta con una copia de la instalación en otro servidor para dar servicio en caso de falla.		Néstor Javier Salazar	Permanente
Desactualización de la información en la intranet, debido al incumplimiento de políticas.	ACEPTABLE	Diariamente se revisa esta información.		Néstor Javier Salazar	Permanente
Daño de un disco duro en el servidor X-Mate - Externo, debido a falta de realización de los mantenimientos preventivos, falla o caida eléctrica, no contar con las condiciones ambientales adecuadas, sabotaje o catástrofe natural.	ACEPTABLE	Los discos estan en mirror y se cuenta con un servidor adicional de back up en caso de daño.		Néstor Javier Salazar	Permanente
Mala utilización del software, debido a que no existe documentación del software desarrollado o adquirido, o que no se dé la adecuada capacitación al cliente interno del sofware desarrollado.	ACEPTABLE	Cuando la situación lo amerite se ofrecerá a los usuarios una capacitación para presentar la nueva funcionalidad; dentro del proceso de desarrollo (P01.IYT) se tiene contemplada la labor de documentación de aplicaciones.	Software Viewletcam, TOADData Modeller, DTU (Repositorio central de documentación)	Humberto Rueda	Eventual

Eliminación errada de cuentas de usuario activos y de procesos críticos, debido a error humano.	ACEPTABLE	Se cuenta con back up tanto de la información cómo del árbol NDS en el caso de NOVELL, para la base de datos los usuarios no tienen objetos en los ambientes de producción, la recreación del usuario es sencilla.		Néstor Javier Salazar	Eventual

ANEXO C: Normatividad de la seguridad de la información.

NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN

Subtítulos	Sinopsis		Cumple		Observaciones
Órganos de gestión 1.	**¿Que es?**	**Consiste**	SI	NO	
Comité de Seguridad Corporativo.	Es un ente encargado de: Mejora continua de la seguridad de la información	Definición: • Objetivos. • Políticas. • Normas. • Actas • Controles… • Entre otras.		X	
Subcomité de Seguridad	Es un ente encargado de: Garantizar la disponibilidad, integridad, confidencialidad y auditabilidad de la información, para evitar su destrucción, modificación.	Elaborar, implantar, revisar y supervisar la evolución de los planes estratégicos de seguridad de la información de la empresa. Evaluar procesos de gestión de la seguridad. Entre otras funciones.		X	Su composición estarán representados, como mínimo, las siguientes áreas: • seguridad de la información (o equivalente dentro de la empresa: seguridad de datos, seguridad informática, etc.) • seguridad integral o seguridad física • sistemas de información. • prevención del fraude • infraestructuras de red y servicios

					• asesoría jurídica Presidido por el Director de Seguridad (o puesto equivalente).
Funciones 1.1					
Identificación y asignación de funciones.	Principales responsabilidades de las personas o áreas que estén identificadas dentro de cada una de las funciones: • Propietario • Responsable de Seguridad • Encargado del Tratamiento	*Propietario: Controles de seguridad aplicables al activo de información. Administrar los mecanismos y medidas de seguridad. *Responsable de Seguridad: Definir los controles de seguridad basándose en la Normativa de Seguridad de la Información y los análisis de riesgos. *Encargado del Tratamiento: Implantar los controles de seguridad, decidir las tecnologías más adecuadas.		X	**Un activo** de información puede ser un sistema de información, una información de naturaleza concreta (información financiera de la empresa, información de los empleados de la empresa, etc.), un sistema que presta un servicio, etc. Aunque es deseable una efectiva segregación de funciones, dependiendo del tamaño de la empresa, circunstancias coyunturales, etc. una misma persona o área podría desempeñar varias funciones de estas simultáneamente, siempre y cuando la propia naturaleza de las funciones a desempeñar simultáneamente lo permita. *Estas funciones serán identificadas, asignadas y a aprobadas por el Subcomité de Seguridad.*

Relación con autoridades y grupos de interés. 1.2					
Relaciones con autoridades y fuerzas	Mantener los contactos necesarios con las autoridades y fuerzas de seguridad del país correspondiente.	Mantener el contacto con las entidades reguladoras en cada país para anticiparse y adecuarse a los cambios legislativos que afecten a la seguridad de forma proactiva.	X		
OBLIGACIONES RELATIVAS AL PERSONAL 2.					
Obligaciones del personal	Las obligaciones de seguridad a las que están sujetos los empleados, proveedores y terceras partes se definirán y documentarán en	En elaborar una Guía de “obligaciones, recomendaciones y consejos de seguridad". *Cumplir con los consejos, recomendaciones,	X		Estas obligaciones aplican tanto al personal que trabaja en la empresa (empleados, proveedores y terceras partes) como al personal que pueda a su vez subcontratar alguno de los anteriores agentes, es decir, las obligaciones en materia de seguridad se deberán cumplir por todas aquellas empresas que sean

	consonancia con la Política y Normativa de Seguridad.	criterios, políticas, procedimientos y normativas de seguridad de la empresa.			subcontratadas. Además de esto se recomienda el buen uso de todos los elementos de trabajo como son: (ordenadores personales, portátiles, PDA's, etc.)
Previo a los contratos. 2.1.					
Verificación del personal	No aplica.				
Obligaciones del personal en los contratos	Ver: **OBLIGACIONES RELATIVAS AL PERSONAL (2.)**				
Durante los contratos 2.2.					
Concienciación, educación y formación en seguridad.	Realizar campañas de concienciación y formación en materia de seguridad de la información a todo el personal de la empresa.	Cursos específicos sobre seguridad de la información acorde con el área: dirección, técnicos, administradores y usuarios de los sistemas.		X	
Procedimiento disciplinario.	Se recomienda definir formalmente un procedimiento disciplinario para	Cuando existan indicios de uso ilícito o abusivo por parte de un empleado, la			ESTO SE ESTA DEFINIDO EN LA

	empleados que hayan cometido una infracción o incumplimiento de seguridad.	empresa realizará las comprobaciones oportunas.	X		POLITICAS DE SEGURIDAD DE LA INFORMACION.
Finalización o cambio de los contratos. 2.3.					
Devolución de activos	Empleados, proveedores y personas de terceras partes deberán devolver todos los activos pertenecientes a la empresa a la finalización del contrato.	Estos activos pueden ser: ordenadores personales, teléfonos móviles, llaves, tarjetas de identificación, soportes informáticos (CDs, discos duros, etc.), tarjetas de crédito, etc.	X		
Cancelación de acceso	Se eliminará el acceso a los sistemas de información y locales de la empresa de los empleados, proveedores y personas de terceras partes que finalicen el contrato.		X		Si el contrato no finaliza pero cambia sustancialmente, se revisará el acceso a los sistemas y locales, eliminándolo si es necesario.

3. CLASIFICACIÓN Y TRATAMIENTO DE LA INFORMACIÓN

Subtítulos	Sinopsis		Cumple		Observaciones
Clasificación de la información. 3.1.	**¿Que es?**	**Consiste**	SI	NO	
Niveles de clasificación.	La información deberá clasificarse de acuerdo a su sensibilidad o grado de impacto en el negocio de la empresa.	• RESERVADA: información de alta sensibilidad. • RESTRINGIDA: acceso controlado un grupo reducido de personas. (áreas, proyectos.) • USO INTERNO: no debe estar disponible externamente. • PÚBLICA: información cuya divulgación no afecte a la empresa.	X		En el anexo A Tabla A.1. REF A.7.2.1 *" la información se debe clasificar en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la organización*" ICONTEC, COMPENDIO Sistema de Gestión de la Seguridad de la Información. (SGSI). p.37.
Responsables de clasificar la	Presidentes, directores	Definir los Niveles de clasificación			

información.	generales, ETC	vistos anteriormente.	X		
Tratamiento de la información clasificada 3.2.					
Inventario de información clasificada	La información RESERVADA o RESTRINGIDA y todos los activos que la tratan serán identificados e inventariados.	Se recomienda utilizar una herramienta para la gestión del registro e inventario de información clasificada.	X		
Propiedad de la información clasificada	La información RESERVADA o RESTRINGIDA y todos los activos que la tratan tendrán designados un propietario responsable del cumplimiento de los controles de seguridad que apliquen a la información.	El propietario de una información clasificada es el empleado (con un cargo directivo o gerencial: gerente, director, etc.) que tiene la decisión sobre la finalidad, contenido y uso de la información.	X		Se recomienda identificar el propietario de todos los activos de información existentes en la empresa, contengan o no información clasificada.
Acceso y uso de información clasificada	El acceso a la información deberá estar autorizado por el propietario de la misma, el cual establecerá los medios necesarios	Definir unas normas generales de uso aceptable de la información en la empresa para empleados, proveedores y	X		

	para que el personal acceda.	terceras partes,			
Etiquetado de información clasificada	La información RESERVADA, RESTRINGIDA, de USO INTERNO o PÚBLICA será identificada de forma que indique su nivel de clasificación.	• etiquetado de información en formato electrónico: correo electrónico, pantallas de aplicaciones, documentos en Word, PowerPoint, etc. • etiquetado de información impresa en papel • etiquetado de soportes informáticos con información clasificada: disquete, CDROM, DVD, cinta, etc.	X		
Almacenamiento de información clasificada	La información RESERVADA será custodiada por el propietario de la misma. La información RESERVADA y RESTRINGIDA en formato electrónico se almacenará cifrada tanto en los sistemas de información como en los soportes informáticos. La información RESERVADA y RESTRINGIDA en soporte impreso se almacenará bajo llave o cualquier otro		X		Los pasos necesarios para almacenar la información clasificada según los criterios anteriores (uso de programas de cifrado, protocolo de custodia de llaves, etc.), se indicarán en el "**Procedimiento de clasificación y tratamiento de información clasificada**" de cada empresa.

	mecanismo que garantice su custodia con total confidencialidad.				
Reproducción de información clasificada	La reproducción o copia de información RESERVADA o RESTRINGIDA (en formato electrónico o impreso) sólo se podrá realizar con autorización expresa del propietario de la información.		X		No se reproducirá información RESERVADA o RESTRINGIDA sin una justificación que atienda a alguna razón de trabajo o negocio, es decir, sólo se reproducirá cuando sea necesaria.
Distribución de información clasificada	La distribución de información RESERVADA o RESTRINGIDA sólo se realizará a las personas previamente autorizada por el propietario de la misma y mediante los controles necesarios que garanticen su confidencialidad e integridad.		X		Los controles y procedimientos deben estar en el manual "**Procedimiento de clasificación y tratamiento de información clasificada**"
Destrucción de información clasificada	La destrucción de información RESERVADA o RESTRINGIDA (en formato electrónico o impreso) se realizará de forma que no se pueda recuperar total o parcialmente por ningún medio físico u electrónico.		X		La destrucción de información RESERVADA y el medio utilizado para su destrucción (p.e, incineración, trituración, rayado, formateo seguro, sobre escritura con ceros o valores nulos, etc.)
Intercambio de información 3.3.					
Intercambio de información	El intercambio formal de información con organizaciones externas deberá estar regulado por un acuerdo que estará en	Criterios y controles definidos en función de los diferentes medios y recursos existentes para el intercambio de información: fax, teléfono, carta,	X		

	consonancia con la legislación aplicable.	correo electrónico, redes de comunicaciones, etc.			
Servicios de comercio electrónico 3.3.1.					
Servicios de comercio electrónico.	Las transacciones on-line de comercio electrónico serán protegidas frente a las amenazas de transmisión incompleta, duplicación, pérdida, alteración o revelación no autorizada.	Se deberán considerar: *requisitos y controles *requisitos de disponibilidad *responsabilidad y seguros. ETC.	X		
identificación y autenticación 3.4.					
Identificación y autenticación	Los usuarios se identificarán y autenticarán en el acceso a los sistemas de información, recursos, áreas de proceso de datos y redes de	Usuario y contraseña • contraseñas de un solo uso. • certificados digitales personales • biometría • tarjetas de acreditación.	X		

	comunicaciones de la empresa.	ETC.			
Identificación 3.4.1.					
Registro de identidad	OBSERVAR El anterior ítem “Identificación y autenticación”				
Identificadores personales	Cada usuario tendrá su propio y único identificador, no permitiéndose que varios usuarios compartan el mismo identificador.	*El identificador no deberá en ningún caso tener privilegios avanzados que supongan un riesgo alto *la excepción será autorizada por el Gestor de Usuarios de la empresa.	X		Es conveniente disponer de un base de datos donde se encuentren registrados los identificadores asignados a los usuarios, con el objeto de no asignar el mismo identificador dos veces.
Unicidad de la identidad corporativa.	Todo usuario tendrá una identidad corporativa que será única en la empresa, no permitiéndose que existan dos identificadores iguales.	Es conveniente que el identificador corporativo del usuario sea el mismo que utiliza para el acceso a los sistemas internos de la empresa en la que trabaja.	X		
	Todos los identificadores de usuarios que no se	Los pasos necesarios para revisar periódicamente los			

Identificadores inactivos	hayan utilizado durante un periodo máximo de 120 días (periodo de inactividad) serán deshabilitados.	usuarios inactivos se indicarán en el "**Procedimiento de registro y gestión de identidades**" de la empresa.	X		
Baja de identificadores	Se eliminarán o deshabilitarán los identificadores de empleados internos y externos que no sigan prestando sus servicios en la misma.	Los pasos necesarios para solicitar y dar de baja un usuario se indicarán en el "**Procedimiento de registro y gestión de identidades**"	X		

3.4.2. Autenticación

Subtítulos	**Sinopsis**		**Cumple**		**Observaciones**
Proceso de autenticación 3.4.2.1	**¿Que es?**	**Consiste**	SI	NO	
Pantalla de autenticación en los sistemas	Las pantallas de presentación de los sistemas de información previas al proceso de autenticación presentarán la mínima información necesaria.	En el acceso a servidores web, etc. No se presentará información sobre el sistema operativo (nombre, versión, etc.) ni de los servidores.		X	Si la autenticación es errónea, el sistema no puede devolver errores del tipo: • el usuario no existe • la contraseña no es válida • no se encuentra el perfil (deduciéndose que el identificador y contraseña son correctos pero no tienen asociado perfil de acceso)

Bloqueo de identificadores	Los identificadores de usuario se bloquearán automáticamente si tienen 5 o más intentos fallidos.	El número de intentos y las ventanas de tiempos pueden ser más restrictivos si se determina en el análisis de riesgos del sistema.	X		
Fecha y hora del último acceso y número de accesos fallidos.	Una vez completado el proceso de autenticación, se presentará al usuario la fecha y hora del último acceso satisfactorio, así como el número de autenticaciones fallidas realizadas desde la fecha.	Con este control el usuario puede conocer si su identificador está comprometido (si hay un acceso posterior al que hizo la persona) o si alguien está intentando entrar con su identificador al sistema.		X	Adicionalmente, se recomienda mostrar al usuario la dirección del equipo desde el que accedió correctamente la ultima vez y las direcciones de los equipos desde los que se intentó acceder fallidamente.
Contraseñas 3.4.2.2					
Gestión de contraseñas	Se definirán procedimientos de gestión de contraseñas en los que se especifique la generación, distribución y cambio de las mismas.		X		La especificación de cómo se generan, distribuyen y cambian las contraseñas que utilizan los usuarios en función del sistemas de información al que pertenecen, se indicará en el "**Procedimiento de registro y gestión de identidades**" de la empresa.
	Las contraseñas iniciales o	El administrador no pueda conocer			Se forzará a los usuarios a cambiar estas

Generación y reinicio de contraseñas.	reiniciadas serán siempre diferentes y aleatorias.	las contraseñas que se comunican a los usuarios.	X		contraseñas iniciales o reiniciadas en el primer acceso o uso de las mismas.
Distribución de contraseñas	No se permitirá la distribución de contraseñas en claro por cualquier red de comunicaciones.	Se recomienda utilizar mecanismos de cifrado para proteger las contraseñas	X		
Periodo y mecanismo de cambio de contraseñas.	Por norma general, se forzará el cambio de aquellas contraseñas que no se hayan cambiado en un periodo mayor a 120 días.		X		Existirán mecanismos que permitan a un usuario el cambio de contraseña a petición del mismo en cualquier momento.
Longitud y sintaxis de contraseñas.	Las contraseñas tendrán un mínimo de 6 caracteres (ocho en el caso de las cuentas de administración).		X		
Almacenamiento de contraseñas.	Las contraseñas no se almacenarán cifradas o mediante funciones resumen con acceso restringido, de forma que se garantice su confidencialidad e integridad.	Los mecanismos de cifrado deben estar basados en estándares públicos de probada fortaleza.	X		
Certificados	Se establecerán procedimientos de registro, generación, distribución,				

digitales personales 3.4.2.3	recuperación, renovación, revocación y destrucción de los certificados digitales asociados a usuarios.				se indicará en el "**Procedimiento de registro y gestión de identidades**"
Almacenamiento de certificados digitales personales.	Las claves privadas de los certificados asociados a usuarios cuyo uso sea la autenticación y firma serán almacenadas en tarjetas o dispositivos criptográficos.				
Validación de los certificados digitales personales	Los sistemas que utilicen mecanismos basados en certificados digitales para identificar y autenticar a los usuarios que acceden, comprobarán la validez, caducidad y no revocación de los certificados.				
3.4.2.4 Generadores dinámicos de contraseñas.					
Generadores dinámicos de contraseñas	Se establecerán procedimientos de activación, distribución, reasignación y desactivación de los generadores dinámicos de contraseñas.	La asignación de cada generador (también llamado "token" o testigo) será individual y personal.			
Biometría	NO APLICA				

3.5. CONTROL DE ACCESO

Subtítulos	Sinopsis		Cumple		Observaciones
Política de control de acceso 3.5.1.	**¿Que es?**	**Consiste**	SI	NO	
Política de control de acceso	Se definirá una política de control de acceso de los usuarios a todos y cada uno de los sistemas de información, recursos, áreas de proceso de datos, servicios y redes de comunicaciones de la empresa.	los criterios o la política de control de acceso general a los sistemas de información, recursos, servicios y redes de comunicaciones de la empresa.	X		La política de control de acceso estará definida en el "**Procedimiento de gestión de accesos de usuarios**" de la empresa.
Gestión de accesos 3.5.2.					
	Se definirán procedimientos formales de solicitud, autorización y revocación de los	Esto se indicará en el "**Procedimiento**			

Gestión de los accesos de los usuarios.	accesos de los usuarios a los sistemas de información, recursos, áreas de proceso de datos, servicios y redes de comunicaciones de la empresa.	**de gestión de accesos de usuarios**" de la empresa.	X		
Gestor de Usuarios	En cada empresa se definirá el Gestor de Usuarios, que será el área o persona encargada de gestionar las solicitudes de acceso de los usuarios (petición de autorizaciones, gestión de permisos, etc).	Gestionar y mantener actualizado el "**Procedimiento de gestión de accesos de usuarios**" de la empresa.	X		Se recomienda que el Gestor de Usuarios de la empresa dependa jerárquica o funcionalmente del área de seguridad del departamento de sistemas de información o de algún área de seguridad definido.
Limitación del periodo de conexión	En aquellos casos en los que sea posible y no afecte a la operatividad de los usuarios, se limitará el acceso a los sistemas de información. (sólo en horario laboral, días laborales, etc).	Este control es adecuado en sistemas de criticidad alta, de acuerdo a un análisis de riesgos previo.	X		

Control de acceso a los sistemas de información 3.5.3.					
Acceso a los sistemas de información	Controlar el acceso mediante mecanismos que garanticen que los usuarios no acceden con privilegios distintos a los autorizados.	los mecanismos de control de acceso sean adaptables a los cambios de la política de control de acceso.	X		Un sistema de información no sólo controlará el acceso de los usuarios sino también el de otros sistemas o aplicaciones que necesiten acceder al mismo.
Perfiles de acceso	Los sistemas de información implementarán perfiles o grupos de acceso.	Los privilegios de acceso a la información y los permisos en los recursos se concederán a perfiles y nunca a usuarios individuales.	X		ALGUNOS PERFILES: • áreas de negocio que utilizan el sistema • administración y operación del sistema • desarrollo y mantenimiento del sistema • gestión de cambios del sistema • administración de seguridad • auditoria de seguridad
Revisión de derechos de acceso	Se revisarán periódicamente los perfiles y privilegios de accesos de los usuarios en los sistemas de información.	"**Procedimiento de revisión de derechos de acceso**" de cada empresa.	X		• los perfiles y privilegios de los usuarios en un sistema de información se revisarán al menos cada 6 meses • siempre que el sistema de información sufra cambios importantes se revisarán los perfiles y privilegios de los usuarios en el sistema
Opciones presentadas al usuario	En la medida de lo posible, los sistemas de información no presentarán al usuario opciones o funcionalidades a	Con este control, además de facilitar el uso de la aplicación, el usuario no ha de conocer opciones que no	X		

	las que no tenga acceso.	debería saber.			
Tiempo de expiración de una conexión	Los sistemas suspenderán las sesiones que tengan un tiempo de inactividad igual o superior a 30 minutos.	Este control es especialmente importante para sistemas con alta criticidad.	X		
Control de acceso a las redes de comunicaciones 3.5.4.					
Control de acceso en la red local.	Los equipos de red controlarán el acceso a la red local de la empresa mediante mecanismos que garanticen que sólo acceden los usuarios y sistemas autorizados.	Se recomienda que los dispositivos (switches, etc.) de red local cableada utilicen mecanismos de autenticación y control de acceso a nivel de puerto.			Se recomienda que se establezcan perfiles de acceso, de forma que en función del usuario que accede, se le asigna una VLAN concreta de acuerdo a su perfil
Control de acceso remoto de los	En el acceso remoto de los usuarios a la red interna (a través de una línea telefónica, Internet, redes inalámbricas externas, extranet,	La robustez y fiabilidad del mecanismo de autenticación que se utilice en cada caso estará en consonancia con la criticidad de la red	X		

usuarios	etc.) se implantarán mecanismos de autenticación y control de acceso robustos ligados al usuario.	y los sistemas e información a la que se pueda acceder.			
Control de acceso remoto de proveedores	El acceso remoto de un proveedor para el mantenimiento o diagnóstico puntual de un sistema interno deberá ser previamente autorizado por el propietario de dicho sistema.		X		Se limitará al tiempo estrictamente necesario para realizar la prestación de servicio establecida.
Control de acceso de puertos de configuración	Se controlará el acceso lógico y físico a los puertos de configuración y diagnóstico de los dispositivos y equipos de red.		X		Muchos equipos de red (routers, switches, etc.) tienen un puerto de administración y monitorización. Estos puertos deben estar deshabilitados cuando no se utilicen y su acceso remoto o físico debe estar restringido.

3.6. REGISTROS DE AUDITORÍA Y MONITORIZACIÓN

Registros de auditoria 3.6.1.					
Generación de registros de auditoria	Se registrarán todos los eventos de seguridad, es decir, todos los sucesos, ocurrencias o fallos observables en un sistema de información o red de comunicaciones que puedan estar relacionados con la	Registrarán la actividad de los administradores y operadores de los sistemas de información.	X		• los eventos requeridos por la legislación aplicable • los intentos de autenticación fallidos • los accesos de los usuarios a los sistemas, tanto autorizados como los intentos no autorizados.

	confidencialidad, integridad o disponibilidad de la información.				
Formato de los registros de auditoria	NO APLICA				
Integridad y confidencialidad de los registros de auditoria	NO APLICA				
Disponibilidad y almacenamiento de los registros de auditoria	NO APLICA.				

3.7. REDES Y COMUNICACIONES

Operación de redes de comunicaciones 3.7.1.					
Procedimientos Operativos de Seguridad de las redes de comunicaciones	Se deben definir, implantar y revisar Procedimientos Operativos de Seguridad (POS) para la gestión de las redes de comunicaciones, dispositivos de encaminamiento (routers) y cortafuegos que forman la red de la	Estos Procedimientos Operativos de Seguridad indicarán los pasos necesarios para la instalación, configuración y gestión segura de las redes de comunicaciones y elementos de red.	X		Todo los procedimientos deben estar documentados.

	empresa.				
Gestión de cambios en las redes de comunicaciones	Se realizará un seguimiento y un control de los cambios en la arquitectura de red de la empresa y en los elementos de red (routers, cortafuegos, switches, etc).	Identificación y registro de los cambios significativos (cambios en las rutas o protocolos de encaminamiento, interconexión de redes. ETC.	X		
Segregación de tareas en la gestión de redes de comunicaciones	Las tareas y responsabilidades propias de gestión de las redes de comunicaciones estarán segregadas para reducir e impedir las oportunidades de acceso no autorizado a la red.	Mediante la segregación de tareas y responsabilidades se debe evitar que una misma persona pueda acceder, modificar o usar una red sin autorización.		X	El control (activación, lectura, almacenamiento, borrado, etc.) de los registros de actividad de la red no deberá estar en manos de la misma persona cuyas acciones originan dichos registros.
Planificación de redes de comunicaciones 3.7.2.					
Planificación de la capacidad de las redes de comunicaciones	Se monitorizará el uso de las redes de comunicaciones con el objetivo de ajustar y planificar la capacidad de las líneas y los	Estas planificaciones deben tener en cuenta los requisitos de tiempo de respuesta en el	X		

	elementos de red (routers, cortafuegos, switches, etc.)	acceso a la información y los sistemas que la tratan, así como la tendencia actual y proyectada del acceso a los recursos.			
Seguridad de la red interna 3.7.3.					
Segmentación de la red interna	La red interna de la empresa se segregará en varios segmentos lógicos de red de acuerdo a unos niveles de riesgo.	Estos segmentos de red se aislarán mediante cortafuegos o dispositivos de encaminamiento (routers), que controlarán el acceso y el tráfico entre los segmentos de acuerdo a unos los criterios y políticas definidos.		X	*si el segmento está dedicado a sistemas de usuarios o a albergar servidores centrales • la criticidad de los sistemas conectados al segmento (y de la información que tratan) • la criticidad de la información que se transmite • la criticidad de los servicios existentes • la exposición potencial a amenazas externas (conexión con Internet, etc.)
Conexiones con redes externas.	Cualquier conexión de la red interna con otras redes externas estará protegida con un cortafuegos.	redes externas, se indicarán en el "**Procedimiento de gestión de cambios e interconexión en las redes de comunicaciones**"			No se permitirá el uso de módems ni otros mecanismos similares (ADSL, etc.) de conexión a redes externas en sistemas que estén conectados a la red interna, a menos que se garantice una conexión segura a dicha red acordada formalmente entre las partes.

	de la empresa.			
Control del encaminamiento y servicios de red.	Se controlará la configuración de encaminamiento y las rutas implementadas en las redes de comunicaciones, de manera que se garantice la correcta implementación de los criterios y políticas que regulan el tráfico permitido entre los segmentos lógicos de red.	X		Este control es necesario para mitigar el riesgo que, en caso de un posible incidente de seguridad, un intruso consiga cambiar las rutas y pueda burlar los filtros implementados en los cortafuegos.
Acceso remoto	En el acceso remoto de los usuarios a la red interna (a través de red telefónica, Internet, etc.) se implantarán mecanismos que comprueben que la seguridad del ordenador personal que se conecta es suficiente y no pone en peligro la seguridad de la red interna.	X		Una vez que la conexión de un usuario finalice, se debe borrar toda la información que pudiera quedar en el ordenador.
Monitorización de la seguridad de red	Las redes de comunicaciones establecerán controles de seguridad para prevenir, registrar y monitorizar las amenazas de la red y proteger de las mismas a los sistemas que hacen uso de la red y la información en tránsito.	X		Se establecerán sistemas de detección/protección de intrusos de red (IDS/IPS de red) para registrar y monitorizar los eventos de seguridad de la red.
Seguridad en los servicios de red	En los acuerdos con los proveedores de servicios de red (conectividad, redes privadas, etc.) se identificarán las funcionalidades y requisitos de seguridad necesarios (cifrado, autenticación, tráfico permitido, etc.), así como los niveles de servicio aceptables.	X		Estos requisitos y niveles de servicio se monitorizarán periódicamente y se tendrá el derecho de auditoria.
Redes inalámbricas	Las redes inalámbricas establecerán mecanismos de seguridad que garanticen	X		Los mecanismos que deben implementar las redes inalámbricas se indicarán en el

	un nivel de protección similar a las redes cableadas.				"**Estándar de seguridad en redes inalámbricas**" de la empresa.
Cifrado de las comunicaciones 3.7.4.					
Cifrado de las comunicaciones	La transmisión de información a través de redes de comunicaciones se cifrará en función de su nivel de clasificación.	La información RESERVADA o RESTRINGIDA por redes de comunicaciones debe estar cifrada.			Se recomienda cifrar el tráfico de gestión de los sistemas de información y de red (mediante SSL, ssh, etc). *Se cifrarán todas las comunicaciones inalámbricas.

3.8. CONTROL DE SOFTWARE

Operación de sistemas 3.8.1.					
Autorización de tratamiento de información	Los sistemas de información que realicen un tratamiento de la información del negocio deberán estar en conocimiento del área de sistemas.	El área de sistemas deberá gestionar estos sistemas (en bases de datos Access, Excel, etc.) e implantar los controles de seguridad como requisito previo a la explotación de los mismos.			
Procedimientos Operativos de Seguridad de los sistemas operativos	Se deben definir, implantar y revisar Procedimientos Operativos de Seguridad para los	Los Procedimientos Operativos de Seguridad indicarán los pasos			Los criterios de seguridad que deben cumplir los sistemas operativos se indicarán en el "**Estándar de seguridad en sistemas operativos**" de la empresa.

	sistemas operativos existentes en los equipos de la empresa.	necesarios para la instalación, configuración y gestión segura de los sistemas operativos.	X		Estos POS (Windows, UNIX, etc.) estarán documentados, publicados y disponibles para los administradores que lo necesiten.
Procedimientos Operativos de Seguridad del software de base	Se deben definir, implantar y revisar Procedimientos Operativos de Seguridad para el software de base existente en los equipos de la empresa.	Dentro del software de base se incluyen las bases de datos, servidores web, servidores de aplicaciones, servidores de correo, ETC.	X		Estos POS estarán documentados, publicados y disponibles para los administradores que lo necesiten.
Gestión de cambios en el software	Se realizará un seguimiento y un control de los cambios en los sistemas operativos y software de base de los sistemas de información.	Cuando se realicen estos cambios, se revisarán los sistemas y aplicaciones críticas para el negocio con el fin de asegurar que el cambio no ha tenido un impacto negativo en los mismos.	X		"**Procedimiento de gestión de cambios y actualización del software**" Se recomienda utilizar una base de datos o herramienta para mantener un inventario de software instalado: versiones instaladas, configuraciones, ubicación, responsable y documentación asociada.
Segregación de tareas en la gestión de sistemas	Las tareas y responsabilidades propias de gestión de los sistemas estarán segregadas para reducir las	Mediante la segregación de tareas se debe evitar que una misma persona pueda acceder, modificar o usar un	X		

	oportunidades de acceso no autorizado, sea involuntario o deliberado.	sistema sin autorización ni posibilidad de detección.			
Aislamiento de sistemas	Los sistemas críticos para el negocio dispondrán de recursos informáticos dedicados aislados del resto, en función de la criticidad de la información.	La decisión de aplicar de este control estará determinada por un análisis de riesgos en la que la criticidad del sistema la determine el propietario del mismo.	X		
Planificación y aceptación de sistemas 3.8.2.					
Planificación de la capacidad de los sistemas	Se monitorizará el uso de los recursos en los sistemas con el objetivo de ajustar y planificar la capacidad de los mismos de acuerdo al rendimiento esperado.	Estas planificaciones deben tener en cuenta los requisitos de los nuevos sistemas, así como la tendencia actual y proyectada del uso de los recursos.	X		
Aceptación de	Se establecerán criterios de aceptación de nuevos sistemas, actualizaciones y	Estos criterios de aceptación deben ser probados en cada nuevo sistema	X		Estos criterios se indicarán en el "**Procedimiento de gestión de cambios y**

sistemas	nuevas versiones, así como las pruebas adecuadas antes de su aceptación.				**actualización del software**"
Adquisición y recepción de software	• estará en consonancia con los procesos de negocio, con la estrategia de plataforma y con la arquitectura y estándares de seguridad • en las solicitudes de propuestas a los distintos proveedores se pedirá como requisito el cumplimiento de los criterios y estándares de seguridad de la empresa.		X		Todo el software deberá ser entregado por el proveedor en soporte ROM o, en su defecto, deberá entregarse por un mecanismo que garantice su integridad.
Protección frente a códigos maliciosos 3.8.3.					
Controles frente a códigos maliciosos	Se implantarán controles de detección, prevención y recuperación frente a códigos maliciosos (virus, caballos de Troya, gusanos, bombas lógicas, etc).	Se controlará la entrada de virus en la empresa en todos los puntos de comunicación con el exterior, tanto en los puntos de entrada compartidos (correo, web, etc.) como en los puntos de entrada locales (disquetera, CDROM, etc).	X		Configuración: Se analizará cualquier fichero existente en los dispositivos de almacenamiento externo que se conecten al sistema (discos duros externos, memorias flash, CDs, DVDs, etc.) Se analizará cualquier fichero descargado (desde Internet o cualquier red) a través del navegador (páginas web, ejecutables, etc.)

Controles frente al uso de códigos de mantenimiento de ordenadores	El uso de códigos móviles y software de gestión centralizada y mantenimiento remoto de ordenadores debe estar previamente autorizado y su configuración será documentada y de acuerdo a unos criterios de seguridad establecidos.	La autorización de uso de un software de gestión centralizada y mantenimiento remoto de ordenadores debe corresponder a los encargados del tratamiento y seguridad de la información.	X		
Dispositivos móviles 3.8.4.					
Seguridad en dispositivos móviles	Se definirán e implantarán los controles necesarios orientados a proteger la información en los dispositivos móviles (ordenadores portátiles, agendas, teléfonos móviles, etc.)	Estos controles serán: • controles de protección física: uso de candados, etc. • controles de acceso lógico: contraseña de arranque (BIOS), uso de tarjeta inteligente, etc.	X		Estos controles serán igualmente aplicables en aquellos ordenadores personales y sistemas que los empleados utilicen para el teletrabajo, sean o no propiedad de la empresa. Se indicarán en el "**Estándar de seguridad en dispositivos móviles**"
Gestión de vulnerabilidades	Se gestionarán las vulnerabilidades que afecten a los sistemas operativos y				

3.8.5.	software de base de forma efectiva y sistemática, minimizando el tiempo de exposición de los sistemas y el riesgo de que puedan ser explotadas.		X		

3.9. DESARROLLO Y MANTENIMENTO DE SISTEMAS

Requisitos de seguridad 3.9.1.					
Análisis de riesgos	Se realizará un análisis de riesgos para cada nuevo sistema de información y en los cambios importantes que se realicen sobre los sistemas.	La identificación de estos controles y requisitos se realizará de acuerdo al "**Procedimiento de valoración de riesgos y controles**"	X		Los requisitos de seguridad deben ser especificados, documentados, justificados y aceptados en las primeras etapas del desarrollo o adquisición de los sistemas. En los análisis de riesgos participarán, al menos, el propietario de los activos, el área de seguridad de la información y los responsables del tratamiento.
Validación en el proceso de datos 3.9.2.					
Validación en la entrada de datos	La entrada de datos en los sistemas y aplicaciones será validada para comprobar si son correctos y adecuados.	Los criterios de validación de entrada de datos se indicarán en el "**Estándar de seguridad en aplicaciones**" de cada empresa.	X		Se establecerán controles de validación en la entrada de datos a través de: • interfaces con otras aplicaciones • formularios on-line de entradas manuales • entradas masivas de datos a través de tareas "batch"
Validación en el	Los sistemas y aplicaciones incluirán controles internos de validación de datos	Los criterios de validación de proceso interno de			

proceso interno de datos	para detectar cualquier corrupción de la información por errores de proceso o actos deliberados.	datos se indicarán en el "**Estándar de seguridad en aplicaciones**"	X		
Integridad en el intercambio de información	Se establecerán mecanismos de integridad y autenticidad en el intercambio de información entre sistemas y aplicaciones.	Los criterios de integridad en el intercambio de información entre sistemas y aplicaciones se indicarán en el "**Estándar de seguridad en aplicaciones**"	X		
Validación en la salida de datos	La salida de datos en los sistemas y aplicaciones será validada para comprobar si son correctos y adecuados.	Los criterios de validación de salida de datos se indicarán en el "**Estándar de seguridad en aplicaciones**"	X		Opcionalmente, las aplicaciones pueden incluir controles de corrección de los datos de salida.
Controles criptográficos 3.9.3.					
Uso de controles	En los sistemas y aplicaciones en los que se considere necesario, se	El uso de controles criptográficos quedará determinado por el análisis de riesgos del sistema, así			

criptográficos en el software	utilizarán controles criptográficos para proteger la información.	como el nivel o fortaleza de los mecanismos de cifrado a utilizar (algoritmos, longitudes de clave mínimas, etc).			
Gestión de claves criptográficas	Se realizará una gestión de todas las claves criptográficas para garantizar la eficacia de los controles criptográficos.				Los pasos necesarios para el registro, generación, distribución, almacenamiento, recuperación, renovación, revocación y destrucción de las claves criptográficas se indicarán en el "**Procedimiento de gestión de claves criptográficas**"
Mantenimiento y gestión de cambios 3.9.4.					
Compatibilidad de los sistemas	Los sistemas desarrollados deben ser compatibles con las infraestructuras de producción homologadas en la empresa.	los sistemas desarrollados han de utilizar las soluciones y servicios comunes de seguridad.	X		• los servicios de identificación, autenticación y control de acceso • los servicios de copias de respaldo ("backup") • los sistemas cortafuegos y las políticas de implementan • los servicios de monitorización de registros de actividad • los servicios de continuidad y contingencia
Gestión de cambios en el desarrollo de	Los cambios en las aplicaciones desarrolladas o adquiridas seguirán un proceso formal de documentación,		X		Este proceso estará integrado con el "**Procedimiento de transferencia de software entre los entornos de desarrollo, pruebas y**

software	especificación, pruebas, control de calidad, implantación y autorización de acuerdo a la metodología de desarrollo e implantación de sistemas de la empresa.			**producción**"
Separación de recursos para los entornos de desarrollo, pruebas y producción	Los entornos de desarrollo, pruebas y producción contarán con sistemas y recursos separados para reducir los riesgos de acceso o cambios no autorizados en el software.	X		Se establecerán reglas para transferir, previa autorización, el software de los sistemas y aplicaciones entre los entornos de desarrollo, pruebas y producción.
Acceso al código fuente	El acceso al código fuente de los sistemas y aplicaciones desarrolladas estará restringido al personal autorizado.	X		
Datos de prueba	En el entorno de desarrollo no se realizarán en ningún caso pruebas con datos reales procedentes del entorno de producción.	X		Los datos serán borrados del entorno de pruebas una vez que las pruebas hayan finalizado, no permaneciendo en ningún caso de forma indefinida.
Puertas traseras	Se establecerán los mecanismos necesarios con el objetivo de prevenir "puertas traseras" en los sistemas y aplicaciones. puertas traseras (malintencionadas o por error de programación)			Estos mecanismos se indicarán en el "**Estándar de seguridad en aplicaciones**" de cada empresa.
Externalización del desarrollo de sistemas.	El desarrollo de sistemas y aplicaciones por terceros será monitorizado y controlado para garantizar la calidad y seguridad del software.	X		• se definirá claramente la propiedad del software desarrollado, los derechos de propiedad intelectual y los acuerdos de licencias

3.10. GESTIÓN DE INCIDENCIAS

Notificación de

incidencias 3.10.1.				
Notificación de incidencias y problemas de seguridad	Se establecerán procedimientos y canales de notificación de incidencias y problemas de seguridad que deberá seguir todo empleado interno o externo que sea consciente de cualquier evento o anomalía que afecte o pudiera afectar a la seguridad de la información o los sistemas que la tratan.	X		Aclaración: aunque en el documento se utilizan indistintamente las palabras "incidente" e "incidencia", se utiliza preferiblemente "incidencia" a cualquier problema o notificación susceptible de ser gestionada, haya causado o no una pérdida en la empresa.
Responsabilidades y procedimientos en el tratamiento de incidencias	Se establecerán los procedimientos y las responsabilidades en la gestión y respuesta a las incidencias de seguridad de la información.	X		las diferentes acciones a realizar en función de la naturaleza y gravedad del incidente, como pueden ser: fallos de sistemas y pérdida de servicio. Código malicioso: propagación de gusanos, etc. Denegación de servicio.
Aprendizaje de los incidentes	Se cuantificarán los tipos, volumen, frecuencia, daños y costes producidos por los incidentes de seguridad con el objetivo de identificar las mejoras y controles necesarios.	X		El análisis y cuantificación de los incidentes de seguridad producidos deberá identificar los controles y mejoras necesarias orientadas a reducir el volumen, la frecuencia, los daños y los costes causados por los mismos.
Recopilación y análisis de evidencias	Las evidencias recopiladas durante la gestión de incidentes deberán ser recolectadas, custodiadas y presentadas de forma que se garantice su integridad y veracidad en todo el proceso y sirvan como pruebas fehacientes, válidas y admisibles en posibles acciones legales.	X		Se tendrá especial atención en la recopilación de registros de auditoría e imágenes de dispositivos de almacenamiento (discos duros, memorias, etc.)

3.11. GESTIÓN Y DISTRIBUCIÓN DE SOPORTES

Gestión de soportes 3.11.1.					
Inventario de soportes	Los soportes informáticos serán inventariados y etiquetados con la información suficiente para su control y localización.	Se mantendrá un registro o inventario con los datos identificativos de cada soporte.	X		Los pasos necesarios para la gestión de este registro se indicarán en el "**Procedimiento de gestión, envío y recepción de soportes de información**"
Almacenamiento de soportes	Los soportes estarán almacenados en áreas de seguridad restringidas al personal autorizado.	Los soportes se almacenarán de acuerdo a los tiempos de conservación de la información que contienen, conforme a los criterios definidos.	X		Los soportes de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura.
Destrucción de soportes	Los soportes que ya no sean necesarios deberán ser destruidos de forma que sea imposible la	La destrucción de un soporte estará marcada por el tiempo de vida del mismo, su utilidad o la necesidad de destruir la	X		Se indicarán en el "**Procedimiento de gestión, envío y recepción de soportes de información**"

	recuperación posterior de la información que contienen.	información que contiene una vez finalizado su tiempo de retención.			
Distribución de soportes 3.11.2.					
Entrada de soportes	Se definirán e implantarán procedimientos de entrada de soportes con información. Se mantendrá un registro de entrada de soportes	• identificador del soporte • tipo de soporte (cinta, DVD, CD, etc.) ENTRE OTRAS.	X		Los pasos necesarios para la recepción de soportes de información, se indicarán en el "**Procedimiento de gestión, envío y recepción de soportes de información**"
Salida de soportes	Se definirán e implantarán procedimientos de salida de soportes con información. Se mantendrá un registro de salida de soportes.	• número de soportes y número de orden que ocupa dentro de dicha serie (si es una serie encadenada) ENTRE OTRAS.	X		En el envío de soportes al exterior se establecerán mecanismos de protección física que garanticen la confidencialidad e integridad de la información y controles que permitan detectar si se ha producido algún acceso no autorizado.

3.12. COPIAS DE RESPALDO Y RECUPERACIÓN

Copias de respaldo 3.12.1.					
Criterios de respaldo y	Se definirán los	La información, se			En este estándar se indicarán como mínimo los

recuperación de la información	criterios de respaldo de la información en consonancia con las necesidades del negocio.	indicarán en el "**Estándar de respaldo y recuperación**" de cada empresa.	X		siguientes parámetros: • los responsables de realizar las copias de respaldo y posterior custodia • periodicidad de las copias de respaldo • número de copias ETC.
Realización de copias de respaldo de la información	Se realizarán copias de respaldo de la información y del software de los sistemas que la tratan de acuerdo a los criterios de respaldo y recuperación de la información que se hayan definido.	Se debe disponer de los dispositivos y procedimientos necesarios para la realización de las copias de respaldo y posterior recuperación en caso de desastre o fallo de los soportes.	X		Los pasos necesarios para la realización de estas copias de respaldo se indicarán en el "**Procedimiento de copias de respaldo y recuperación**"
Recuperación de la información 3.12.2.					
Recuperación de información	La recuperación de información a partir de copias de respaldo deberá ser autorizada por el propietario de la misma.	Se registrarán las actuaciones que se realicen de recuperación de información, las personas que ejecuten el proceso, los datos restaurados y el motivo de la recuperación.	X		En este procedimiento se incluirán los procesos de validación relacionados con la operación y la aceptación del propietario de la información o sistema recuperado.

3.13. CONTINUIDAD DE NEGOCIO

Responsabilidades 3.13.1.				
	Se establecerán planes de contingencia			Cada servicio, recurso o activo de información

Necesidad y responsabilidades	para reducir el impacto provocado por una paralización total o parcial de la capacidad operativa de la empresa y garantizar la recuperación ágil y progresiva de los servicios, procesos y recursos de negocio afectados. La elaboración del plan de contingencia de un servicio o recurso la realizará el responsable o propietario del mismo.		X		deberá estar englobado dentro del alcance de un plan de contingencia. En caso contrario, el responsable del servicio, recurso o activo debe elaborar un plan de contingencia
Planes de contingencia 3.13.2.					
Análisis de impacto	Se realizará un análisis de impacto dentro de cada plan de contingencia que se realice.	En cada análisis se involucrará a los propietarios de los recursos, servicios y activos incluidos dentro del alcance del plan.	X		• Se identificarán los recursos críticos incluidos en el alcance del plan de contingencia. Los recursos críticos son aquellos cuya pérdida, deterioro o paralización ocasionaría pérdidas y daños en el negocio.
Implantación y desarrollo de los planes de contingencia	En la implantación y desarrollo de los planes de contingencia se establecerán las estrategias de respaldo, los equipos de emergencia, los procedimientos y los planes de actuación necesarios para garantizar la recuperación de los servicios, procesos y recursos críticos de la empresa dentro de los parámetros de tiempo y calidad aceptables para el negocio.		X		En todo el proceso de implantación y desarrollo de los planes de contingencia se garantizará la seguridad de los datos y sistemas incluidos dentro del alcance.
Estructura de los	Los planes de contingencia existentes en una empresa se estructurarán de forma consistente y relacionada, de				• los planes de contingencia existentes en la empresa y la relación entre los mismos • los responsables y las personas involucradas

planes de contingencia	modo que un plan de contingencia englobará e incluirá los planes de contingencia de rango o alcance inferior y al mismo tiempo, se englobará y supeditará a los planes de contingencias de rango o alcance superior.	X		de cada plan de contingencia • los recursos incluidos en el alcance de cada plan de contingencia
Pruebas, mantenimiento y revisión de los planes de contingencia	Los planes de contingencia se probarán, actualizarán y revisarán regularmente para comprobar su eficacia y actualización.	X		• Se definirá un plan de pruebas, en el que se identificará la planificación de las pruebas, el alcance y los resultados esperados de cada prueba, así como el personal involucrado en las mismas y los recursos necesarios.

3.14. TERCERAS PARTES EXTERNAS

Acceso de terceras partes 3.14.1.					
Identificación de riesgos con terceras partes	Cuando existan terceras partes que por razones de negocio necesiten acceder a la información o a los sistemas que la procesan, se identificarán los riesgos e implantarán los controles necesarios.	Los controles necesarios que se identifiquen en el análisis de riesgos serán incluidos en los acuerdos con las terceras partes	X		• El tipo de acceso que se necesita: físico (oficinas, áreas de proceso de datos, etc.), lógico (aplicaciones, bases de datos, etc.), red (acceso remoto, conexiones permanentes entre oficinas, etc.), si la información a la que se accede está en la empresa o fuera de la empresa (en las instalaciones de la terceras parte)
	Se identificarán los	• restricción de			• procedimiento de notificación y gestión de

Seguridad en el acceso de clientes	requisitos de seguridad en el acceso de los clientes a la información y los sistemas de la empresa.	copias y no divulgación de la información • productos y servicios que se proveen.	X		incidentes de seguridad • declaración del derecho de monitorización de las actividades de los clientes por parte del prestador del servicio • cláusulas de protección de datos de carácter personal • derechos de propiedad intelectual y patentes
Acuerdos con terceras partes.	Los acuerdos con terceras partes involucradas en el acceso, procesamiento, comunicación o tratamiento de la información o sistemas que la procesan incluirán los requisitos de seguridad que sean aplicables.		X		En la Política Corporativa de Seguridad de la Información, se regula que las relaciones con entidades colaboradoras deben estar amparadas siempre por los contratos de prestación de servicios correspondientes, incluyendo cláusulas de garantías en el uso de la información.
Acuerdos de confidencialidad	La relación con terceras partes involucradas en el tratamiento de la información estará regulada con acuerdos o cláusulas de confidencialidad y no divulgación. Estos acuerdos deberán ser identificados y revisados periódicamente.		X		Los acuerdos de confidencialidad y no divulgación deben cumplir con las leyes y regulaciones aplicables en cada país.
Prestación de servicios de terceras partes 3.14.2.					
Prestación de servicios por terceros	Se controlará que se cumplen, implantan, gestionan y mantienen los controles de seguridad, los servicios prestados y el nivel de servicio definidos en los acuerdos con terceras partes.		X		La responsabilidad y el control de los servicios prestados por una tercera parte será de los jefes de proyecto y/o directores de área que hayan contratado el servicio.
Monitorización y revisión de los servicios prestados por terceros	Los servicios, informes y registros facilitados por las terceras partes que prestan un servicio serán monitorizados y revisados periódicamente.		X		El control de los servicios prestados por un tercero no debe confiar sólo en las evidencias e informes de nivel de servicio ofrecidos por el proveedor, ya que estos pueden estar manipulados en su conveniencia.

Gestión de los cambios de los servicios prestados por terceros	Los cambios en los servicios prestados por terceras partes serán gestionados identificando los riesgos e implantado y revisando los controles de seguridad necesarios.	X		Los cambios en los servicios prestados por terceros pueden implicar cambios necesarios en la organización (modificación o revisión de los procedimientos de seguridad, nuevos requisitos y controles, etc.) o cambios en la tercera parte (uso de nuevas tecnologías, cambios en la plataforma, cambios en las redes, etc).
Selección de proveedores	NO APLICA			

3.15. SEGURIDAD FÍSICA Y DEL ENTORNO

Áreas de seguridad 3.15.1.				
Perímetros de seguridad física	Se utilizarán perímetros de seguridad física para proteger las áreas en las que se localice la información y los sistemas que la tratan.	X		Un perímetro de seguridad física es un elemento que supone una barrera física (muros, puertas de control con tarjeta, puestos de control de personas, etc). Los perímetros de seguridad estarán regulados por la normativa y procedimientos de seguridad física de cada empresa.
Controles físicos de entrada	Las áreas de seguridad estarán protegidas por controles de entrada que aseguren el acceso sólo al personal autorizado.	X		Los controles físicos de entrada estarán regulados por la normativa y procedimientos de seguridad física de cada empresa.
Protección de despachos, oficinas y recursos	NO APLICA			
Protección frente a amenazas externas	NO APLICA			

del entorno				
Trabajo en áreas de seguridad	NO APLICA			
Protección de los equipos 3.15.2.				
Instalación y protección de equipos	Los equipos deberán situarse y protegerse para reducir el riesgo de amenazas del entorno (agua, fuego, etc.) así como las oportunidades de accesos no autorizados.	X		La protección física de los equipos estará regulada por la normativa y procedimientos de seguridad física de cada empresa.
Fallos en el suministro	Los equipos se protegerán frente a fallos eléctricos y otras anomalías en el suministro necesario (agua, ventilación, aire acondicionado, etc).	X		La continuidad del suministro necesario para los equipos estará regulada por la normativa y procedimientos de seguridad física de cada empresa.
Protección del cableado	El cableado de energía y telecomunicaciones que porten datos o soporten servicios de información se protegerán contra interceptación o daños.	X		La protección del cableado estará regulada por la normativa y procedimientos de seguridad física de cada empresa.
Mantenimiento de equipos	En los locales donde se encuentren ubicados los equipos existirán controles ambiéntales adecuados de temperatura y humedad, de manera que los equipos se mantengan adecuadamente para asegurar su continua integridad y disponibilidad.	X		El mantenimiento físico de los equipos estará regulado por la normativa y procedimientos de seguridad física de cada empresa.
Protección de los equipos fuera de los locales de la empresa	Se establecerán medidas de protección física para los equipos fuera de los locales de la empresa, teniendo en cuenta los riesgos de trabajar fuera de dichos locales.	X		Las medidas de protección física de los equipos fuera de los locales de la empresa estarán reguladas por la normativa y procedimientos de seguridad física de cada empresa.
Protección en la reutilización y	En todos los elementos de los equipos que contengan dispositivos de			Las medidas orientadas a garantizar el borrado de datos y licencias en la reutilización y

eliminación de equipos	almacenamiento de datos se comprobará que todo dato sensible y software bajo licencia se ha borrado o sobrescrito antes de su reutilización o eliminación.	X		eliminación de equipos estarán reguladas por la normativa y procedimientos de seguridad física de cada empresa.
Salida de equipos	Los equipos no deben salir de los locales de la empresa sin previa autorización.	X		Los procedimientos de autorización de salida de equipos estarán regulados por la normativa y procedimientos de seguridad física de la empresa.

3.16. CONFORMIDAD

Conformidad legal 3.16.1.					
Legislación aplicable	El tratamiento de la información cumplirá con los requisitos de la legislación vigente del país en el que se trate en materia de seguridad de la información.		X		Se identificarán los requisitos de las leyes aplicables en el tratamiento y seguridad de información y se definirán los responsables internos de velar por su cumplimiento.
Derechos de propiedad intelectual	El uso de software, productos y material protegido por derechos de propiedad intelectual cumplirá con las restricciones definidas en la legislación aplicable y en las licencias de uso.		X		
Legislación sobre protección y retención de registros de auditoria	NO APLICA				
Legislación sobre protección de datos de carácter personal	El tratamiento de información con datos de carácter personal cumplirá con los requisitos de la legislación y contratos	Se debe definir una política de protección y privacidad de datos de carácter personal de la empresa y	X		

	aplicables, implantando las medidas oportunas de acuerdo al nivel de seguridad de los datos.	comunicarla a todos los empleados.			
Legislación sobre monitorización del abuso de sistemas y redes	La monitorización del uso que los usuarios realizan de los sistemas de información y redes de comunicaciones de la empresa cumplirá con los requisitos de la legislación aplicable.	Los empleados internos y externos serán informados de sus obligaciones y limitaciones en el uso de los sistemas de información y redes de comunicaciones de la empresa.	X		La monitorización del cumplimiento de estas obligaciones y limitaciones por parte de la empresa deberá cumplir con las leyes de protección al honor y derecho a la intimidad de las personas, secreto de las comunicaciones, etc.
Legislación sobre criptografía.	El uso de controles criptográficos cumplirá con los requisitos de la legislación aplicable.				Especialmente tienen relevancia las leyes en materia de firma electrónica e importación o exportación de tecnología (software y hardware) de cifrado, así como las leyes que reservan a los órganos gubernamentales métodos de acceso a la información cifrada
Conformidad normativa y revisión del cumplimiento 3.16.2.					
Revisión independiente de la organización y estrategia de seguridad	La organización y estrategia en seguridad de la información en cada central serán revisadas por una entidad independiente del área auditada.				NO APLICA

Revisión independiente del cumplimiento normativo	El cumplimiento de la Normativa de Seguridad de la Información en cada central será revisado de forma periódica por una entidad independiente del área auditada.			NO APLI CA
Revisión independiente de la seguridad los sistemas y redes de comunicaciones	La seguridad de los sistemas de información y redes de comunicaciones será revisada por una entidad independiente del área auditada.			NO APLICA