IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA EN LA CONFEDERACIÓN DE CÁMARAS DE COMERCIO - CONFECÁMARAS

JESÚS DAVID TABARES RENDÓN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ D. C.

2015

JESÚS DAVID TABARES RENDÓN

PROYECTO DE GRADO PARA OPTAR AL TÍTULO DE ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Asesor: MARTÍN CAMILO CANCELADO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D. C.
2015

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Bogotá, Octubre, 3, 2015

A todos los genios que permitieron que la seguridad informática se convirtiera en una pasión, a mi hermana BIT y a mi novia EMF, a ambas gracias por su amor y apoyo incondicional.

AGRADECIMIENTOS

Gracias a la Universidad Nacional Abierta y a Distancia por enseñarnos que el compromiso y la responsabilidad no es cuestión de edificios, ni limitaciones de espacio y tiempo.

CONTENIDO

LISTA DE TABLAS

LISTA DE GRÁFICAS

LISTA DE ANEXOS

RESUMEN

Consolidación de los documentos fundamentales para la puesta en marcha de un Sistema de Gestión de la Seguridad Informática en la Confederación Colombiana de Cámaras de Comercio - Confecámaras.

Se deja establecido de igual forma cual es el grado de compromiso de toda la Confederación en el alcance de su misión y visión estratégica en lo relativo a su seguridad y al aseguramiento de todos sus procesos, activos y recursos humanos.

INTRODUCCIÓN

La relevancia que la Confederación Colombiana de Cámaras de Comercio ha alcanzado a nivel nacional, la ha llevado a ser depositaria de amplia confianza por parte de diversas entidades del estado, llevando a la entrega de proyectos de gran envergadura y repercusión nacional.

Es por eso que, Confecámaras al ser una empresa de tecnología que pretende consolidar y afianzar sus servicios y procesos, debe recurrir a la aplicación de una norma que le permita no sólo entender y controlar sus procesos sino que mediante la gestión y aplicación de buenas prácticas mejore su prestigio ante sus clientes y brinde confianza a sus futuros proyectos.

Conocedores de los anterior, una norma como la ISO 27001 en su versión 2013, brindará una sólida base no sólo a los proyectos actuales, sino una confiable plataforma de acción y gestión, todo apalancado en la seguridad de la información.

1. OBJETIVOS

1.1.1 OBJETIVO GENERAL

Implementar bajo la norma ISO 27001 un Sistema de Gestión de Seguridad de la Información que genere un ambiente de seguridad y confianza en los procesos informáticos de la Confederación de Cámaras de Comercio de Colombia - Confecámaras.

1.1.2 OBJETIVOS ESPECÍFICOS

- Definir que procesos se llevan a cabo en las áreas de Infraestructura y Servicios Tecnológicos y que no se encuentran acordes a prácticas seguras en el manejo de la información.

- Especificar mediante el método de análisis y gestión de riesgos estructurados Magerit, el estado actual y fallas en los procesos que se ejecutan a diario dentro de la organización.

- Incrementar el nivel de seguridad de la información de la entidad mediante la implementación de las políticas de seguridad en la Confederación de Cámaras de Comercio.

1.2 PLANTEAMIENTO DEL PROBLEMA

1.2.1 DEFINICIÓN DEL PROBLEMA

La Confederación Colombiana de Cámaras de Comercio actualmente agrupa a las 57 Cámaras de Comercio del País y recientemente ha ampliado su portafolio a diferentes entidades como los bancos y las aseguradoras con servicios de centralización de información y gestión integral de la misma. Para ser más exactos, Confecámaras para 42 Cámaras de Comercio a través de su área de servicios tecnológicos, provee un catálogo de servicios tecnológicos centralizados, distribuidos y mixtos; entregando de esta manera Software y Plataforma como servicio en diferentes proyectos tipo ERP, gestión documental y principalmente programas de control registral.

En la actualidad y ante el auge del internet y de conceptos como el “cloud”, la Confederación ha iniciado un proceso de centralización muy ambicioso que pretende en última instancia agrupar en una fuente de alta confiabilidad y calidad al 42% de la información registral del territorio Colombiano.

Por lo anterior y con el ánimo de gestionar de una manera responsable toda la información que ha sido delegada a la Confederación, además de blindar en la mayor medida posible todos los procesos, se hace indispensable contar en primera instancia, con una base de conceptos y de políticas que procuren en cada aspecto seguridad y confiabilidad a través de lo que se denomina SGSI – Sistema de Gestión de Seguridad Informática, el cuál comprende un conjunto de políticas de administración de la información. El término fue acuñado principalmente por la ISO/IEC 27001 y aunque no es la única normativa que utiliza este término o concepto, sí es la norma que más se acomoda a las necesidades de protección de la información en la Confederación Colombiana de Cámaras de Comercio - CONFECÁMARAS.

Los SGSI se caracterizan por tener para las organizaciones diversas fases como son: el diseño, la implantación, y el mantenimiento dentro de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, comprometiendo a la integridad y garantizando la disponibilidad de todos los activos referentes a la información, y sin ir más allá, minimizando de manera decisiva los riesgos de seguridad de la información.

De manera sustancial, un Sistema de Gestión de Seguridad de la Información debe cumplir de manera eficiente por un periodo de tiempo extenso calculado y de esta forma va adaptándose a los cambios internos de la organización, incluso a los

factores externos del entorno y de esta manera adquiere mayor madurez e influye de manera contundente en las Cámaras de Comercio del territorio Colombiano.

1.2.2 JUSTIFICACIÓN

Partiendo de la idea y de la necesidad de consolidar en cuestiones de seguridad, todos los servicios tecnológicos de la Confederación Colombiana de Cámaras de Comercio, se hace necesario la implementación de un Sistema de Gestión de Seguridad de la Información a través de la norma ISO 27001 en su versión 2013, la cual brindará una sólida base no sólo a los proyectos actuales, sino una confiable plataforma de acción y gestión para los proyectos futuros, todo enmarcado bajo estándares mundiales de seguridad.

Como retribución al buen nombre que la Confederación se ha labrado, el día 30 de mayo de 2014, entró en vigencia la Circular Externa 005 emitida por la Superintendencia de Industria y Comercio y entregó nuevas pautas para la operación registral en Colombia a través del Sistema Preventivo de Fraudes – SIPREF, el cual tiene como finalidad prevenir que terceros ajenos a los titulares de los registros públicos que se llevan en las Cámaras de Comercio, modifiquen la información que allí reposa y se administra.

Dicho modelo de prevención incrementará la seguridad y confiabilidad en la operación de los registros públicos, y posee de manera implícita las siguientes ventajas:

- Verificar la identidad de las personas que realizan trámites físicos o electrónicos.

- Prevenir que terceros no autorizados por el titular del registro modifiquen la información que figura en los registros públicos de las Cámaras de Comercio.

- Prevenir fraudes en los registros de los comerciantes o inscritos que no han actualizado datos o no han efectuado su renovación en los últimos tres (3) años.
- Utilizar un sistema de alertas que ponga en conocimiento del comerciante o inscrito la presentación de un trámite y a su vez la inscripción o devolución del mismo.
- Permitir a los titulares de la información registral adoptar medidas que detengan conductas fraudulentas.

Para dar mayor peso a la seguridad y confiabilidad del proyecto SIPREF se está adelantando ante la Registraduría General de la Nación un proyecto mediante el

cual se permitirá a las Cámaras de Comercio del territorio colombiano consumir un servicio web que brindará la posibilidad de validar la identidad como ciudadano colombiano, esto mediante la lectura del documento de identidad y/o de la lectura biométrica de su índice derecho. La validez de dicho proyecto estará dada siempre y cuando se pueda demostrar un sistema de gestión de seguridad implementado en la Confederación Colombiana de Cámaras de Comercio y a su vez la extensión de las políticas que lo conforman para las Cámaras de Comercio del país a las cuales Confecámaras brinda soporte tecnológico.

1.3 MARCO TEÓRICO

La Aplicación de modelos y estándares dentro de lo concerniente a la seguridad de la información se encuentra enmarcada dentro de una norma internacional puntual denominada ISO/IEC 27001 la cuál es un estándar para la seguridad de la información (Information technology - Security techniques – Information security management systems - Requirements) aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission. La implantación de ISO/IEC 27001 en una organización es un proyecto que suele tener una duración entre 6 y 12 meses, dependiendo del grado de madurez en seguridad de la información y el alcance, entendiendo por alcance el ámbito de la organización que va a estar sometido al Sistema de Gestión de Seguridad de la Información elegido. En general, es recomendable la ayuda de consultores externos. Aquellas organizaciones que hayan adecuado previamente de forma rigurosa sus sistemas de información y sus procesos de trabajo a las exigencias de las normativas legales de protección de datos (p.ej., en España la conocida LOPD y sus normas de desarrollo, siendo el más importante el Real Decreto 1720/2007, de 21 de diciembre de desarrollo de la Ley Orgánica de Protección de Datos) o que hayan realizado un acercamiento progresivo a la seguridad de la información mediante la aplicación de las buenas prácticas de ISO/IEC 27002, partirán de una posición más ventajosa a la hora de implantar ISO/IEC 27001.

El equipo de proyecto de implantación debe estar formado por representantes de todas las áreas de la organización que se vean afectadas por el SGSI, liderado por la dirección y asesorado por consultores externos especializados en seguridad informática generalmente Ingenieros o Ingenieros Técnicos en Informática, derecho de las nuevas tecnologías, protección de datos y sistemas de gestión de seguridad de la información (que hayan realizado un curso de implantador de SGSI). Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) según el conocido como “Ciclo de Deming”: PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 27002, anteriormente conocida como ISO/IEC 17799, con

orígenes en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la British Standards Institution (BSI).

Otro modelo de amplia aplicación y que se ha ganado un papel muy importante dentro de los modelos de sistemas de gestión, se denomina: COBIT (Objetivos de Control para Tecnología de la Información y Relacionados) o por sus siglas en inglés: Control Objectives for Information and related Technology, y trata de un modelo diseñado y creado por el Instituto de Gobierno de Tecnologías de Información (ITGI – Information Technology Governance Institute) perteneciente a la Asociación para la Auditoría y Control de Sistemas de Información (ISACA – Information Systems Audit and Control Association) para el gobierno de las tecnologías de información. Estos códigos de buenas prácticas, están basados en los estándares de seguridad de la información y de gerencia de proyectos más usados en el mundo y en las recomendaciones de cientos de expertos en la materia. El objetivo principal de COBIT es Investigar, desarrollar, publicar y promocionar un conjunto de objetivos de control. Generalmente, estos son aceptados para las tecnologías de información que sean autorizadas, actualizadas y aplicadas internacionalmente para el uso del día a día de los gestores de negocios y también auditores. Esto es logrado a partir de la definición de “34 procesos de acuerdo, a las áreas de responsabilidad de planear, construir, ejecutar y monitorear, ofreciendo una visión de punta.

Un modelo menos conocido y que ha sido adaptado de modelos internacionales, es el denominado, ISO/IEC, Código de buenas prácticas para la gestión de la seguridad de la información. Creada a partir de la norma británica 7799-1. Ésta norma proporciona recomendaciones a partir de las mejores prácticas en la gestión de la seguridad de la información, dirigida a todos los interesados y responsables de iniciar, implantar o mantener sistemas de gestión de la seguridad (SGSI), partiendo de los conceptos de Confidencialidad, Integridad y Disponibilidad de la información. Se espera que en el transcurso de 2007, esta norma pase a ser parte de la serie de estándares 27000, como la ISO/IEC 27002. La norma inicia con la definición de seguridad de la información y por qué ésta es importante en las organizaciones de hoy en día. Luego propone una manera de establecer los requisitos de seguridad a través de tres fuentes que brindan información acerca de la mayor parte de necesidades de las compañías, la valoración de riesgos de la organización, los requisitos legales (en el caso colombiano aplicaría la ley 527 de 1999, el código disciplinario único y el código penal, y la última fuente está formada por los principios, objetivos y requisitos que hacen parte del tratamiento de la información que la organización ha desarrollado para apoyar sus operaciones.

Como última referencia se encuentra el modelo, “PMBOK” la cual es básicamente una guía de los Fundamentos de la Dirección de Proyectos y establece los Fundamentos de la Dirección de Proyectos. Se establecen entonces que estos constituyen en la suma de conocimientos en la profesión de dirección de

proyectos. La finalidad principal de esta guía es identificar el subconjunto de Fundamentos de la Dirección de Proyectos, generalmente reconocido como buenas prácticas, entendiéndose dicha definición desglosada como: “Identificar” significa proporcionar una descripción general en contraposición a una descripción exhaustiva. “Generalmente reconocido” significa que los conocimientos y las prácticas descritos son aplicables a la mayoría de los proyectos, la mayor parte del tiempo, y que existe un amplio consenso sobre su valor y utilidad. “Buenas prácticas” significa que existe un acuerdo general en que la correcta aplicación de estas habilidades, herramientas y técnicas puede aumentar las posibilidades de éxito de una amplia variedad de proyectos diferentes. “Buenas prácticas” no quiere decir que los conocimientos descritos deban aplicarse siempre de forma uniforme en todos los proyectos; el equipo de dirección del proyecto es responsable de determinar lo que es apropiado para cada proyecto determinado. Cuando se trata de la atención de incidentes en seguridad informática, es de vital importancia la identificación de los riesgos que están latentes en los activos de información de las empresas.

1.4 MATERIALES Y MÉTODOS

1.4.1 METODOLOGÍA

Toda la información recolectada fue capturada y tabulada en los formatos que Magerit presenta como alternativas para sus diagnósticos. A través de los mismos se obtuvieron las salvaguardas y se estimó un real estado de todos los procesos de la Confederación discriminando cada una de sus vertientes.

Es de destacar que las diferentes áreas, poseen un líder que trae consigo toda la experiencia que dan años de manejo y gestión dentro de la organización.

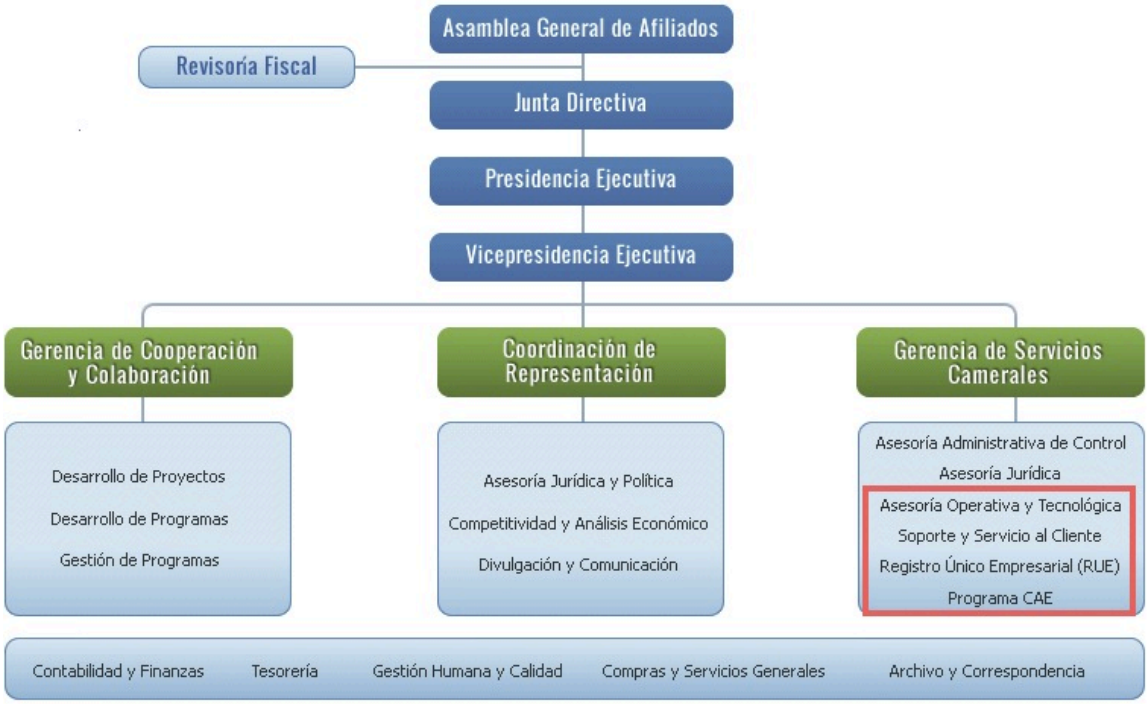
Por tal motivo en dichos elementos se concentrará la mayor parte del trabajo de recolección y será un punto de análisis muy importante para el desarrollo del proyecto del SGSI en la Confederación

1.5 DESARROLLO DEL PROYECTO

1.5.1 ORGANIGRAMA INSTITUCIONAL

El siguiente es el Organigrama institucional (Gráfica 1), publicado y mantenido desde el año 2012. Se enmarca en rojo las áreas correspondientes a las Tecnologías de la Información:

Gráfica 1: Organigrama institucional



Fuente: Pagina Web Confecámaras

El área de informática está compuesta por los siguientes cargos:

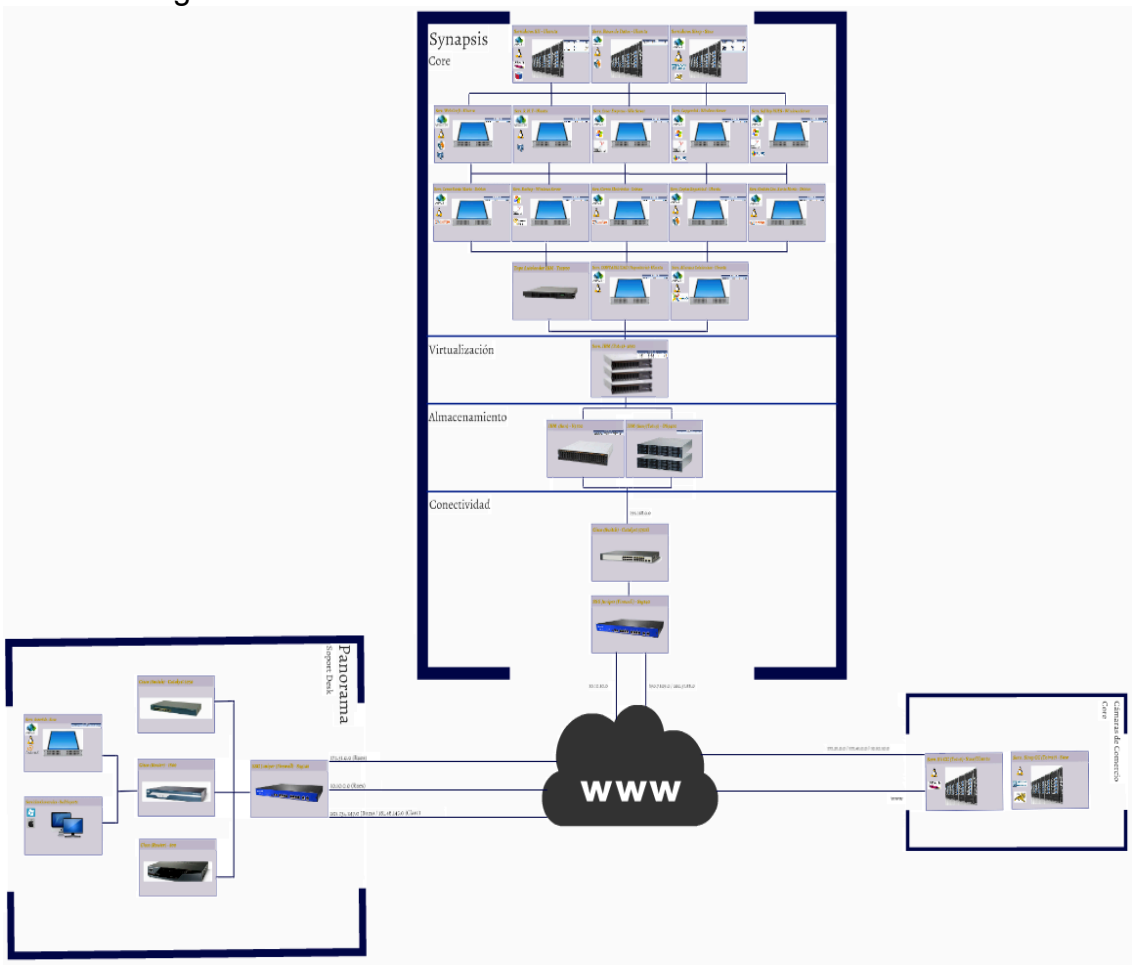
- Jefe de Operaciones
- Analista de operaciones
- Analista de soporte: 1 Nivel
- Analista de soporte: 2 Nivel
- Analista de soporte: 3 nivel
- Coordinador de infraestructura

Los procesos que se adelantan actualmente dentro del área de informática son los siguientes:
Servicios tecnológicos: La Confederación administra y responde por las siguientes plataformas tecnológicas de misión crítica utilizadas por la Red de Cámaras de Comercio y por la propia confederación. La lista de aplicaciones es la siguiente:

- Sirep (Software para registros)
- Sistema Integrado de Información – SII
- Portal CAE (Creación de Empresas)
- Registro Nacional de Turismo (RNT)

El detalle de la gestión del servicio tecnológico ofrecido por Confecámaras se ilustra a continuación en la gráfica 2:

Gráfica 2: Diagrama de infraestructura Confecámaras



Fuente: El autor

2. ALCANCE

La Confederación Colombiana de Cámaras de Comercio establece como principal alcance de su Sistema de Gestión de Seguridad Informática al área de servicios tecnológicos en donde reposa su segundo pilar estratégico de operación:

“Servicios para la Red de Cámaras de Comercio – Atiende la prestación de servicios de alto impacto y nuevos negocios con el convencimiento de la importancia y el potencial de la información de las Cámaras de Comercio.”

Lo anterior se da porque dentro de dicho proceso misional, la Confederación abarca la prestación de sus servicios tecnológicos a las Cámaras de Comercio con

las cuales ha suscrito convenio de tecnología y por ende garantizar dichos servicios es un objetivo que no permite aplazamiento.

La prestación de los servicios principales de tecnología están dispuestos en un Datacenter denominado “Tivit-Synapsis” tipo Tier III, en la zona franca de Fontibón en la ciudad de Bogotá y en el mismo están albergados la mayoría de los activos tipo hardware y servicios que se brindan en calidad de “nube” a los clientes de la Confederación y es donde avanza el “core” del negocio y los servicios críticos.

Continuando, con el primer alcance y dentro del conjunto de actividades que permiten alcanzar un óptimo tratamiento del riesgo, se tendrá en cuenta que dicho análisis llegará hasta la detección primaria del riesgo residual con el ponderado de efectividad estimado a criterio del líder del SGSI y el consecuente cálculo del riesgo inherente, lo anterior como una determinación inicial del estado del sistema de gestión, antes de iniciar su plan de implementación de controles y su estimación posterior a la valoración real del mismo.

Como segundo alcance se establece la seguridad en la prestación del servicio y es el factor humano el que predomina. Por lo tanto el subsecuente alcance del SGSI estará enfocado en controlar en la mayor medida de lo posible toda actividad susceptible de convertirse en una amenaza y así mismo dar un valor agregado desde el recurso humano a toda la operación y en especial a la garantía sobre la prestación eficiente y eficaz de la misma. La referenciación de este alcance estará dada por la ubicación de la oficina de Confecámaras en el edificio Panorama desde la cual se ofrecen los servicios y en donde reside su gestión operativa.

Como último alcance y como parte de la visión de Confecámaras: “Propiciar la competitividad y el desarrollo regional a través del fortalecimiento de las cámaras como instituciones y la representación proactiva del sistema ante el Estado en temas de competitividad, formalización, emprendimiento e innovación empresarial.” Se presenta que Confecámaras a través de su experiencia en la creación de su Sistema de Gestión de Seguridad de la Información desea ser un multiplicador de su conocimiento y propiciar en un futuro cercano la creación de Sistema de Gestión de Seguridad de la Información para sus allegados y adscritos que redunde en un fortalecimiento de todos los eslabones de la cadena de trabajo Cameral y rinda sus frutos descritos como cooperativismo y colaboración.

3. POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

3.1. INTRODUCCIÓN AL DOCUMENTO DE POLÍTICAS

Con el ánimo de mejorar la estrategia de Seguridad de la información de la Confederación Colombiana de Cámaras de Comercio. En adelante Confecámaras, surge la necesidad de buscar un modelo base que permita alinear los procesos hacia un mismo objetivo de seguridad en el manejo de la información.

Para tal fin, se establece una Política de la Seguridad de la Información, como marco de trabajo de la organización en lo referente al uso adecuado de los recursos, buscando niveles adecuados de protección y resguardo de la información, definiendo sus lineamientos, para garantizar el debido control y minimizar los riesgos asociados.

3.2. OBJETIVO DE LAS POLÍTICAS DE SEGURIDAD

Este documento formaliza el compromiso de la dirección frente a la gestión de la seguridad de la información y presenta de forma escrita a los usuarios de sistemas de información el compendio de acciones con las cuales Confecámaras establece las normas para proteger de posibles riesgos de daño, pérdida y uso indebido de la información, los equipos y demás recursos informáticos de la Entidad, los cuales están en constante cambio y evolución de acuerdo con el avance de la tecnología y los requerimientos de la Entidad.

El presente documento tiene como objetivo definir los lineamientos que debe seguir Confecámaras con relación a la seguridad de la Información. Estos lineamientos están escritos en forma de políticas.

3.3. ALCANCE DE LAS POLÍTICAS DE SEGURIDAD

El documento de Política de Seguridad de la Información reglamenta la protección y uso de los activos de información de Confecámaras, y por tanto está dirigido a todos aquellos usuarios que posean algún tipo de contacto con estos activos. Los usuarios de los activos de información de la Entidad deberán diligenciar un acuerdo de confidencialidad, que los compromete con el cumplimiento de las políticas de seguridad aquí descritas. Los usuarios de los activos de información de la Entidad se han clasificado así:

- Colaboradores de Planta: se definen como colaboradores de planta aquellas personas que han suscrito un contrato laboral con la Entidad.

- Funcionarios de Confecámaras: Se definen como los empleados de Confecámaras que son susceptibles de manipular el sistema de autenticación biométrica en línea.

- Contratistas: se definen como contratistas a aquellas personas que han suscrito un contrato con la Entidad y que pueden ser:

- Colaboradores en Misión;
- Colaboradores por Outsourcing: son aquellas personas que laboran en la Entidad y tienen contrato con empresas de suministro de servicios y que dependen de ellos;
- Personas naturales que prestan servicios independientes a la Entidad;
- Proveedores de recursos informáticos.

• Entidades de Control
- Procuraduría;
- Revisoría Fiscal;
- Contraloría General de la República;
- Superintendencia de Industria y Comercio.
- Firmas Auditoras Externas.

• Otras Entidades
- DIAN;

3.4. REQUISITOS LEGALES Y/O REGLAMENTARIOS

Para la implementación de la estrategia de seguridad de la información, Confecámaras debe regirse por lo dispuesto en el marco jurídico y normativo aplicable a las Cámaras de Comercio o entidades que las regulan y aglutinan.

3.5. DEFINICIONES

Para los propósitos de este documento se aplican los siguientes términos y definiciones:

- Activo: Cualquier bien que tenga valor para la organización.
- Acuerdo de Confidencialidad: Es un documento que debe suscribir todo usuario con el objeto de lograr el acceso a recursos informáticos de Confecámaras.
- Administradores: Usuarios a quienes Confecámaras ha dado la tarea de administrar los recursos informáticos y poseen un identificador que les permite tener privilegios administrativos sobre los recursos informáticos de Confecámaras quienes estarán bajo la dirección de la Vicepresidencia de tecnología y soluciones de información de la Entidad.
- Amenaza: Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización.
- Backup: Copia de la información en un determinado momento, que puede ser recuperada con posterioridad.
- Coordinación de Planeación e Innovación: Es el responsable de velar por el cumplimiento de esta Política, documentar el Manual de Seguridad de la Información, los procesos, procedimientos, instructivos y formatos

específicos alineados al estándar internacional ISO 27001 y sus normas derivadas además de los otros marcos generalmente aceptados como: COBIT, ITIL, NIST, ASNZ y DRII, así como liderar la implementación de los controles exigidos por la Ley y la Regulación Vigente.

- Comité de Seguridad: Equipo de trabajo conformado por el Vicepresidente Ejecutivo. Gerente del RUES, Gerente de Servicios Camerales, Director de Desarrollo y Jefe de Servicios Tecnológicos.
- Contraseña: Clave de acceso a un recurso informático.
-
- Control: Medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.
- Directrices: Descripción que aclara lo que se debería hacer y cómo hacerlo, para alcanzar los objetivos establecidos en las políticas.
- Servicios de procesamiento de información: Cualquier servicio, infraestructura o sistema de procesamiento de información o los sitios físicos que los albergan.
- Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no-repudio y confiabilidad pueden estar involucradas.
- Evento de seguridad de la información: Un evento de seguridad de la información es la presencia identificada de un estado del sistema, del servicio o de la red que indica un posible incumplimiento de la política de seguridad de la información, una falla de controles, o una situación previamente desconocida que puede ser pertinente para la seguridad.
-
- Firewall: Conjunto de recursos de hardware y software que protegen recursos informáticos de accesos indebidos.
- Incidente de seguridad de la información: Está indicado por un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- Información confidencial (CONFIDENCIAL): Información generada por Confecámaras y las Cámaras de Comercio que operan a través de Confecámaras y que debe ser conocida exclusivamente por un grupo autorizado de funcionarios por esta. El acceso a este tipo de información debe ser restringido y basado en el principio del menor privilegio. Su divulgación a terceros requiere permiso del titular de la misma y de acuerdos de confidencialidad. Así mismo, su divulgación no autorizada puede causar daños importantes a la Entidad. Todo material generado durante la creación de copias de este tipo de información (ejemplo, mala calidad de impresión), debe ser destruido.

- Información privada (USO INTERNO): Información generada por Confecámaras y las Cámaras de Comercio que operan a través de Confecámaras, que no debe ser conocida por el público en general. Su divulgación no autorizada no causa grandes daños a la Entidad y es accesible por todos los usuarios.
- Información pública: Es la información administrada por Confecámaras y las Cámaras de Comercio que operan a través de Confecámaras que está a disposición del público en general; por ejemplo la información de los registros públicos y la información vinculada al Registro Único Empresarial y Social – RUES.
- LAN: Grupo de computadores y dispositivos asociados que comparten un mismo esquema de comunicación y se encuentran dentro de una pequeña área geográfica (un edificio ó una oficina).
- Licencia de Software: Es la autorización o permiso concedido por el dueño del programa al usuario para utilizar de una forma determinada y de conformidad con unas condiciones convenidas. La licencia precisa los derechos (de uso, modificación, o redistribución) concedidos a la persona autorizada y sus límites, además puede señalar el lapso de duración y el territorio de aplicación.
- Copyright: Son el conjunto de derechos de exclusividad con que la ley regula el uso de una particular expresión, de una idea o información. En términos más generalizados se refiere a los derechos de copia de una obra (poemas, juegos, trabajos literarios, películas, composiciones musicales, grabaciones de audio, pintura, escultura, fotografía, software, radio, televisión, y otras formas de expresión de una idea o concepto), sin importar el medio de soporte utilizado (Impreso, Digital), en muchos de los casos la protección involucra un periodo de duración en el tiempo. En muchos casos el copyright hace referencia directa a la protección de los derechos patrimoniales de una obra.
- Propiedad Intelectual: Es una disciplina normativa que protege las creaciones intelectuales provenientes de un esfuerzo, trabajo o destreza humana, dignos de reconocimiento jurídico.
-
- Derechos patrimoniales: Los derechos patrimoniales de una obra referencia a la forma en cómo se puede utilizar, o recibir algún tipo de beneficio de la obra. Es un derecho temporal, expropiable disponible, renunciable, y embargable.
- Derecho moral: Es la relación intangible que une al creador de una obra y su obra, es un derecho inalienable, nadie puede expropiar ese derecho.
- Open Source (Fuente Abierta): Es el término por el que se conoce al software que es distribuido y desarrollado de forma libre, en el cual la licencia específica el uso que se le puede dar al software.

- Software Libre: Software que una vez obtenido puede ser usado, copiado, modificado, o redistribuido libremente, en el cual la licencia expresamente especifica dichas libertades.
- Software pirata: Es una copia ilegal de aplicativos o programas que son utilizados sin tener la licencia exigida por ley.
- Software de Dominio Público: Tipo de software en que no se requiere ningún tipo de licencia y cuyos derechos de explotar, usar, y demás acciones son para toda la humanidad, sin que con esto afecte a su creador, dado que pertenece a todos por igual. En términos generales software de dominio público es aquel en el cual existe una libertad total de usufructo de la propiedad intelectual.
- Freeware: Software de computador que se distribuye sin ningún costo, pero su código fuente no es entregado.
- Shareware: Clase de software o programa, cuyo propósito es evaluar por un determinado lapso de tiempo, o con unas funciones básicas permitidas. para adquirir el software de manera completa es necesario un pago económico.
- Módem (Modulador - Demodulador de señales): Elemento de comunicaciones que permite transferir información a través de líneas telefónicas.
- Monitoreo: Verificación de las actividades de un usuario con respecto a los recursos informáticos de Confecámaras.
- OTP (One Time Password): Contraseña entregada por el administrador de un recurso informático que permite el primer acceso a dicho recurso y obliga al usuario a cambiarla una vez ha hecho este acceso.
- Plan de contingencia: Plan que permite el restablecimiento ágil en el tiempo de los servicios asociados a los Sistemas de Información de Confecámaras en casos de desastres y otros casos que impidan el funcionamiento normal.
- Política: Toda intención y directriz expresada formalmente por la dirección.
- Protector de pantalla: Programa que se activa a voluntad del usuario, ó automáticamente después de un tiempo en el que no ha habido actividad.
- Proxy: Servidor que actúa como puerta de entrada a la Red Internet.
- Recursos informáticos: Son aquellos elementos de tecnología de Información tales como: computadores servidores de aplicaciones y de datos, computadores de escritorio, computadores portátiles, elementos de comunicaciones, elementos de los sistemas de imágenes, elementos de almacenamiento de información, programas y datos.
- Riesgo: Combinación de la probabilidad de un evento y sus consecuencias.
- Análisis de Riesgos: Uso sistemático de la información para identificar las fuentes y estimar el riesgo.
- Evaluación de Riesgos: Todo proceso de análisis y valoración del riesgo.
- Valoración del riesgo: Proceso de comparación del riesgo estimado frente a criterios de riesgo establecidos para determinar la importancia del riesgo.

- Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- Router: Equipo que permite la comunicación entre dos o más redes de computadores.
- Sesión: Conexión establecida por un usuario con un Sistema de Información.
- Sistema de control de acceso: Elementos de hardware o software que autorizan o niegan el acceso a los recursos informáticos de acuerdo con políticas definidas.
- Sistema de detección de intrusos (IDS): Es un conjunto de hardware y software que ayuda en la detección de accesos ó intentos de acceso no autorizados a los recursos informáticos de Confecámaras.
- Sistema de encripción: Elementos de hardware o software que permiten cifrar la información, para evitar que usuarios no autorizados tengan acceso a la misma.
- Sistema multiusuario: Computador y su software asociado, que permiten atender múltiples usuarios a la vez a través de las redes de comunicación.
- Sistema operativo: Software que controla los recursos físicos de un computador.
- Sistema sensible: Es aquel que administra información confidencial ó de uso interno que no debe ser conocida por el público en general.
- Tercera parte: Persona u organismo reconocido por ser independiente de las partes involucradas, con relación al asunto en cuestión.
- Usuario: toda persona que pueda tener acceso a un recurso informático de Confecámaras
- Usuarios de red y correo: Usuarios a los cuales Confecámaras les entrega un identificador de cliente para acceso a sus recursos informáticos.
- Usuarios externos: Son aquellos clientes externos que utilizan los recursos informáticos de Confecámaras a través de Internet ó de otros medios y tienen acceso únicamente a información clasificada como pública.
- Usuarios externos con contrato: Usuarios externos con los cuales Confecámaras establece un contrato y a quienes se da acceso limitado a recursos informáticos de uso interno.
- Vulnerabilidad: Debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas.

6. RESPONSABLE

6.1. COMPROMISO DE LA DIRECCIÓN

La dirección debe brindar evidencia de su compromiso con el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de los mecanismos para asegurar información:

- Mediante el establecimiento de una política de seguridad de la información;
- Asegurando que se establezcan objetivos y planes de seguridad de la información;
- Estableciendo funciones y responsabilidades de la seguridad de la información;
- Comunicando a la organización la importancia de cumplir los objetivos de seguridad de la información, las responsabilidades legales, y la necesidades de la mejora continua;
- Asegurando que se realizan auditorías internas.

3.6.2. GESTIÓN DE LOS RECURSOS

- Asegurar que las políticas de seguridad de la información brindan apoyo a los requisitos del negocio;
- Identificar y atender los requisitos legales y reglamentarios, así como las obligaciones de seguridad contractuales;
- Mantener la seguridad suficiente mediante la aplicación correcta de todos los controles implementados;
- Asegurar que todo el personal tiene conciencia de la importancia de la seguridad de la información.

3.7. PROCEDIMIENTO

Los miembros del Comité de Seguridad, conscientes que los recursos de información son utilizados de manera permanente por los usuarios de Confecámaras que implementen el servicio de identificación biométrica, definidos en este documento, han considerado oportuno transmitir a los mismos las normas de comportamiento básicas en la utilización de los equipos de cómputo y demás recursos tecnológicos y de información.

Las políticas de seguridad informática tienen como objetivo reducir el riesgo de incidentes de seguridad y minimizar su efecto. Establecen las reglas básicas con las cuales la organización debe operar sus recursos informáticos. El diseño de las políticas de seguridad informática está encaminado a disminuir y eliminar muchos factores de riesgo, principalmente la ocurrencia.

3.7.1. POLÍTICA DE SEGURIDAD DE CONFECÁMARAS.

En Confecámaras se reconoce abiertamente la importancia de la seguridad de la información así como la necesidad de su protección para constituir un activo estratégico de la organización y todas las partes interesadas, el no uso adecuado de los activos de información puede poner en peligro la continuidad del negocio o al menos suponer daños muy importantes que afecten el normal funcionamiento de los procesos.

Los funcionarios, terceros y usuarios en general deberán conocer el presente documento, normas, reglas, estándares y procedimientos que apliquen según las funciones que realicen para la organización, el desconocimiento que conlleve a la violación de lo anteriormente mencionado representará para la persona involucrada las sanciones disciplinarias que apliquen según el incidente presentado.

Igualmente se implementarán los controles de seguridad encaminados a garantizar la confidencialidad, integridad y disponibilidad de los activos de información de Confecámaras con el objetivo de lograr un nivel de riesgo aceptable de acuerdo con la visión, misión, planeación y estrategia de la compañía, y dando cumplimiento al marco jurídico aplicable a los estándares nacionales.

3.7.2. POLÍTICAS GENERALES DE SEGURIDAD INFORMÁTICA

Estas normas son de obligatorio cumplimiento por parte de todos los usuarios de recursos informáticos y se han clasificado en:

- Políticas de Cumplimiento y Sanciones
- Políticas de uso de recursos informáticos.
- Políticas de contraseñas.
- Políticas de uso de la información.
- Políticas del uso de Internet y correo electrónico.
- Políticas de uso de la Intranet y Sitio Web de Confecámaras
- Políticas Generales de la Presidencia.
- Políticas para Desarrolladores de Software.
- Políticas para Administradores de Sistemas.
- Políticas de Copias de respaldo.
- Políticas de Uso de Firewall.
- Políticas para Usuarios Externos.
- Políticas de Acceso Físico.

3.7.3. POLÍTICAS DE CUMPLIMIENTO Y SANCIONES

3.7.3.1. Cumplimiento con la seguridad de la información

Todos los colaboradores de la organización, así como los contratistas, deben cumplir y acatar el manual de políticas y los procedimientos en materia de protección y seguridad de la información. Corresponde velar por su estricto cumplimiento a la Presidencia de Confecámaras y al comité de seguridad.

3.7.3.2. Medidas disciplinarias por incumplimiento de políticas de seguridad

Cualquier incumplimiento de una política de seguridad de la información por parte de un funcionario de contratistas, así como de Confecámaras, estándar, o procedimiento es causa para iniciar acciones disciplinarias, las cuales de acuerdo

a su gravedad pueden suponer la terminación de la vinculación laboral del empleado o contratista.

Si el incumplimiento se origina en una sede, Confecámaras podrá suspender la prestación del servicio de identificación biométrica.

3.7.4. POLÍTICAS DE USO DE RECURSOS INFORMÁTICOS
7.4.1. Instrucciones para el uso de recursos informáticos.

El uso del computador personal y demás recursos informáticos por parte del empleado, trabajadores o usuarios del sistema de autenticación biométrica en línea, debe someterse a todas las instrucciones técnicas, que imparta el comité de seguridad.

3.7.4.2. Uso personal de los recursos

Los recursos informáticos de Confecámaras, dispuestos para la operación registral de la cámaras de comercio, o propios de las cámaras de comercio, solo deben ser usados para fines laborales, entre los cuales, se resalta la prestación del servicio de autenticación biométrica en línea a los usuarios de Confecámaras y las cámaras de comercio usuarias de este servicio. El producto del uso de dichos recursos tecnológicos será de propiedad de la Entidad y estará catalogado como lo consagran las políticas de la Entidad. Cualquier otro uso está sujeto a previa autorización de la Presidencia.

3.7.4.3. Acuerdo de confidencialidad

Para el uso de los recursos tecnológicos de Confecámaras y las cámaras de comercio, todo usuario debe firmar un acuerdo de confidencialidad y un acuerdo de Seguridad de los sistemas de información antes de que le sea otorgado su Login de acceso a la red y sus respectivos privilegios o medios de instalación de las soluciones de autenticación biométrica en línea con su respectivo kit de hardware

- Prohibición de instalación de software y hardware en los computadores de Confecámaras y las cámaras de comercio.

La instalación de hardware o software, la reparación o retiro de cualquier parte o elemento en los equipos de computación o demás recursos informáticos solo puede ser realizada por los funcionarios de sistemas autorizados por Confecámaras y las cámaras de comercio.

3.7.4.4. Uso del aplicativo entregado.

Confecámaras ha suscrito con los fabricantes y proveedores un contrato de "LICENCIA DE USO" para los aplicativos que utiliza. Está terminantemente prohibido copiar cualquiera de los aplicativos que se aloja en los computadores de la Entidad, esto se asegura con la firma del Acuerdo de Confidencialidad para los usuarios y con la firma del contrato realizado con los proveedores que maneje información de uso restringido a Confecámaras Adicional a esto cada usuario, dependiendo de las actividades que realice sobre las aplicaciones maneja un perfil limitado, de esta forma es controlado el acceso.

7.4.5. El usuario es responsable por toda actividad que involucre su identificación personal o recursos informáticos asignados.

Todo usuario es responsable por todas las actividades relacionadas con su identificación. La identificación no puede ser usada por otro individuo diferente a quien fue otorgada dicha identificación. Los usuarios no deben permitir que otros usuarios realicen labores bajo su identidad. De forma similar, los usuarios no deben realizar actividades bajo la identidad de alguien más. La utilización de los recursos informáticos por parte de terceras personas con conocimiento o consentimiento del usuario, o por su descuido o negligencia, lo hace responsable de los posibles daños que estas personas ocasionen a los equipos o a la propiedad de Confecámaras y las cámaras de comercio.

7.4.6. Declaración de reserva de derechos de Confecámaras

Confecámaras y las cámaras de comercio usan controles de acceso y otras medidas de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información manejada por computadores y sistemas de información. Para mantener estos objetivos Confecámaras y las cámaras de comercio se reservan el derecho y la autoridad de: 1. Restringir o revocar los privilegios de cualquier usuario; 2. Inspeccionar, copiar, remover cualquier dato, programa u otro recurso que vaya en contra de los objetivos antes planteados; y, 3. Tomar cualquier medida necesaria para manejar y proteger los sistemas de información de Confecámaras y las cámaras de comercio. Esta autoridad se puede ejercer con o sin conocimiento de los usuarios, bajo la responsabilidad del comité de seguridad siempre con el concurso de la Presidencia o de quién él delegue esta función.

7.4.7. Recursos compartidos.

Está terminantemente prohibido compartir los discos duros o las carpetas de los computadores de escritorio, aunque estén protegidos por contraseña. Cuando exista la necesidad de compartir recursos esto se debe hacer con autorización previa y restringir por Dominio.

3.7.4.8. Todo monitoreo debe ser registrado e informado al jefe inmediato del usuario.

Un usuario puede ser monitoreado bajo previa autorización del comité de seguridad.

3.7.4.9. Acceso no autorizado a los sistemas de información de la Entidad.

Está totalmente prohibido obtener acceso a sistemas de información a los que no se tiene privilegios y de alguna forma dañar o alterar la operación de dichos sistemas. Esto implica la prohibición de capturar contraseñas, llaves de encripción y otros mecanismos de control de acceso que le puedan permitir obtener ingreso a sistemas no autorizados.

3.7.4.10. Posibilidad de acceso no implica permiso de uso.

Los usuarios no deben leer, modificar, copiar o borrar información perteneciente a otro usuario sin la debida autorización de este.

3.7.4.11.Prohibición a la explotación de vulnerabilidades de seguridad de los recursos informáticos.

A no ser que exista una aprobación por escrito para ello o sea parte de su función laboral, los usuarios no deben explotar las deficiencias de seguridad de los sistemas de información para dañar los sistemas o la información contenida en ellos, obtener acceso a recursos a los cuales no se le ha dado acceso. En el caso de encontrar vulnerabilidades, estas deben ser reportadas de inmediato al comité de seguridad.

3.7.4.12. Dejar sistemas sensibles desatendidos.

Si el usuario está conectado a un sistema que contiene información sensible, éste no debe dejar el computador desatendido sin cerrar primero la sesión iniciada.

3.3.7.4.13. Notificación de sospecha de pérdida, divulgación ó uso indebido de información sensible.

Cualquier incidente de Seguridad debe reportarse por escrito al correo electrónico del comité de seguridad.

3.7.4.14. Etiquetado y presentación de información de tipo confidencial a los usuarios de computadores.

Toda la información que sea crítica para la organización debe ser etiquetada de acuerdo a los niveles establecidos en el presente documento: USO INTERNO y CONFIDENCIAL.

3.7.4.15.Traslado de equipos debe estar autorizado.

Ningún equipo de cómputo debe ser reubicado o trasladado dentro o fuera de las instalaciones de Confecámaras y las cámaras de comercio sin previa autorización. Así mismo, ningún equipo de cómputo asignado en el kit de identificación biométrica debe ser reubicado o trasladado de las instalaciones de la sede a la cual fue asignado. El traslado de los equipos se debe hacer con las medidas de seguridad necesarias, por el personal de sistemas autorizado.

3.7.4.16.Control de recursos informáticos entregados a los usuarios.

Cuando un usuario inicie su relación laboral con Confecámaras y las cámaras de comercio se debe diligenciar el documento de entrega de inventario.

Cuando un empleado termine su vinculación laboral con la Entidad, sea trasladado a otra dependencia o por alguna otra circunstancia deje de utilizar el computador personal o el recurso tecnológico suministrado con carácter permanente, deberá hacerse una validación de lo entregado por el usuario contra lo registrado en el formato de descargue de inventario (Firmado). El empleado será responsable de los deterioros o daños que por su negligencia haya ocasionado a los equipos de hardware.

Cuando un funcionario de Confecámaras inicie su relación laboral se debe diligenciar el documento de entrega de inventario.

3.7.4.17. Configuración de sistema operativo de las estaciones de trabajo.

Solamente los funcionarios del área técnica de sistemas están autorizados para cambiar la configuración del sistema operativo de las estaciones de trabajo de los usuarios.

3.7.4.18.Uso restringido de módems en las estaciones de trabajo.

Queda prohibido el uso de módems en las estaciones de trabajo que permitan obtener una conexión directa a redes externas como Internet a menos que se cuente con aprobación escrita por parte de Presidencia.

7.4.19. Protección por Defecto de Copyright

Todos los colaboradores de Confecámaras deben revisar, e investigar los derechos de propiedad intelectual para todo material como libros, artículos, informes, imágenes, software y/o sitio Web encontrado en Internet antes de ser usado para cualquier propósito con el fin de asegurar el cumplimiento de las leyes que aplican para este tipo de información.
Regularmente se deben realizar actividades de monitoreo sobre el software instalado en cada uno de los equipos de la organización, lo anterior para asegurar

que los programas instalados correspondan correctamente con las licencias adquiridas por la empresa.

3.7.4.20. Custodia de Licencias de Software

Las licencias deben ser custodiadas y controladas por el área de tecnología. Esta área debe realizar auditorías de licencia de software como mínimo una vez al año generando las evidencias respectivas, lo anterior para garantizar que los funcionarios solo tienen instalado software legal y autorizado por el jefe de cada área.

3.7.4.21. Apagado de equipos en la noche

Con fin de proteger la seguridad y distribuir bien los recursos de la empresa, los equipos de cómputo deben quedar apagados cada vez que no haya presencia de funcionarios en la oficina durante la noche.

3.7.4.22. Tiempo limitado de conexión en aplicaciones de alto riesgo

Si el usuario está conectado a un sistema que contiene información sensible, y este presenta un tiempo de inactividad corto la aplicación deberá cerrar la sesión iniciada por el usuario.

3.7.5. POLÍTICAS DE USO DE LAS CONTRASEÑAS
3.7.5.1. Confidencialidad de las contraseñas.

La contraseña que cada usuario asigna para el acceso a los sistemas de información, debe ser personal, confidencial e intransferible. Cada usuario debe velar porque sus contraseñas no sean vistas y aprendidas por otras personas.

3.7.5.2. Uso de diferentes contraseñas para diferentes recursos informáticos.

Para impedir el compromiso de múltiples recursos informáticos, cada usuario deberá utilizar diferentes contraseñas para cada recurso al que tiene acceso. Esto involucra así mismo a los equipos de comunicación (firewall, routers, servidores de control de acceso) y a los administradores de los mismos.
3.
7.5.3. Identificación única para cada usuario.

Cada usuario tendrá una identificación única en cada sistema al que tenga acceso, acompañado de un elemento para su autenticación (contraseña) de carácter personal y confidencial para la utilización de los recursos tecnológicos necesarios para sus labores. Esta política rige para aplicativos implementados hasta la fecha de liberación de este documento. En caso del sistema de autenticación biométrica en línea, el acceso al sistema se realizará mediante un cotejo biométrico, los

funcionarios contarán con una identificación única personal y su respectiva contraseña asignada por el encargado por el área de tecnología de Confecámaras.

3.7.5.4. Cambios periódicos de contraseñas.

Todos los usuarios deben ser automáticamente forzados a cambiar su contraseña por lo menos una vez cada 30 días.

3.7.5.5. Longitud mínima de contraseñas.

Todas las contraseñas deben tener una longitud mínima de OCHO (8) caracteres que debe cumplir con algunas de las siguientes características: Incluir combinación de números, letras mayúsculas, minúsculas y caracteres especiales. Este tamaño debe ser validado por el sistema en el momento de generar la contraseña para impedir un tamaño menor.

3.7.5.6. Contraseñas fuertes.

Las contraseñas no deben ser nombres propios ni palabras del diccionario, debe ser una mezcla de números, letras y caracteres especiales.

3.7.5.7. Prohibición de contraseñas cíclicas.

No se debe generar contraseñas compuestas por una combinación fija de caracteres y una combinación variable pero predecible. Un ejemplo de este tipo de contraseñas prohibidas es “Enero-2004” que según la política “Contraseñas fuertes”, es una contraseña válida, pero al mes siguiente pasa a ser “Febrero-2004” y así sucesivamente.

3.7.5.8. Las contraseñas creadas por usuarios no deben ser reutilizadas.

El usuario no debe generar una contraseña idéntica o sustancialmente similar a una que ya haya utilizado anteriormente. Esta política es complementada por la política “Prohibición de contraseñas cíclicas”.

3.7.5.9. Almacenamiento de contraseñas.

Ninguna contraseña debe ser guardada de forma legible en archivos “batch”, scripts, macros, teclas de función de terminal, archivos de texto, en computadores o en otras ubicaciones en donde personas no autorizadas puedan descubrirlas o usarlas. Ningún usuario bajo ninguna circunstancia está autorizado para tener su contraseña en cualquier medio impreso, con excepción de lo contemplado en la política “Almacenamiento de contraseñas de administrador”.

3.7.5.10. Sospechas de compromiso deben forzar cambios de contraseña.

Toda contraseña deberá ser cambiada de forma inmediata si se sospecha o se conoce que ha perdido su confidencialidad.
3.
7.5.11. Revelación de contraseñas prohibidas.

Bajo ninguna circunstancia está permitido revelar la contraseña a empleados o a terceras personas. La contraseña personal no debe ser digitada en presencia de terceras personas, así sean funcionarios de la Entidad. Ningún usuario deberá intentar obtener contraseñas de otros usuarios, excluyendo lo contemplado en la política “Auditoria periódica a las contraseñas de los usuarios”.

3.7.5.12. Bloqueo estación de trabajo.

Todas las estaciones de trabajo de los usuarios deben tener activado el bloqueo automático de estación, el cual debe activarse luego de un período de ausencia o inactividad de 3 min. Por otra parte el escritorio del equipo de trabajo debe estar despejado y ordenado, de tal forma que la información que se encuentre en el puesto de trabajo o en la pantalla (escritorio) del equipo sea estrictamente la suficiente y necesaria para la labor desempeñada.

3.7.5.13. Reporte de cambio en las responsabilidades de los usuarios al Administrador del Sistema I.

El ingeniero en soporte y web master debe reportar por medio de un correo electrónico, de manera oportuna al área de sistemas, todos los cambios significantes en las responsabilidades de un usuario, de su estado laboral, de su ubicación dentro de la organización, con el fin de mantener el principio de seguridad de la información.

3.7.6. POLÍTICAS DE USO DE LA INFORMACIÓN
3.7.6.1. Divulgación de la información manejada por los usuarios de Confecámaras

Confecámaras podrá divulgar la información de un usuario almacenada en los sistemas de acuerdo con la autorización suscrita por él mismo, por disposición legal, por solicitud de autoridad judicial o administrativa salvo las excepciones indicadas en este documento y las disposiciones legales de protección de datos personales.

3.7.6.2. Transferencia de datos solo a organizaciones con suficientes controles.

Confecámaras puede transmitir información privada solamente a terceros que por escrito se comprometan a mantener dicha información bajo controles adecuados de protección. Se da una excepción en casos en los que la divulgación de información es forzada por la ley.

3.7.6.3. Registro de las compañías que reciben información privada.

El personal de Confecámaras que liberó información privada a terceros debe mantener un registro de toda divulgación y este debe contener qué información fue revelada, a quién fue revelada y la fecha de divulgación.

3.7.6.4. Transferencia de la custodia de información de un funcionario que deja Confecámaras

Cuando un empleado se retira de Confecámaras, su jefe inmediato debe revisar tanto los archivos magnéticos, correo electrónico como documentos impresos para determinar quién se encargará de dicha información o para ejecutar los métodos para la destrucción de la información.
3.
7.6.5. Transporte de datos sensibles en medios legibles.

Si se transporta información sensible en medios legibles por el computador (disquetes, cintas magnéticas, CD, memorias USB), la información deberá ser encriptada, siempre y cuando el receptor acepte el intercambio de datos cifrados. Para equipos portátiles este tipo de información es asegurada mediante una aplicación de cifrado.

3.7.6.6. Datos sensibles enviados a través de redes externas deben estar encriptados.

Si se ha de transmitir datos sensibles a través de cualquier canal de comunicación externo, dichos datos deben ser enviados en forma encriptada, siempre y cuando el receptor tenga los recursos necesarios y acepte el intercambio de datos cifrados.

3.7.6.7. Clasificación de la Información

- Todos los activos deben estar claramente identificados y se debe elaborar y mantener un inventario de todos los activos importantes.
- Toda la información y los activos asociados con los servicios de procesamiento de la información deben ser “propiedad” de una parte designada de Confecámaras y las cámaras de comercio.
- Se deben identificar, documentar e implementar las reglas sobre el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de la información.

- Cualquier uso de servicio de procesamiento de información debe ser autorizado por la Gerencia de RUES, y el Gerente de TI de las cámaras de comercio según el caso, por lo anterior cualquier acceso a un servicio no autorizado es prohibido y de esto deben tener conocimiento todos los usuarios involucrados.

3.7.6.8. Eliminación Segura de la Información en Medios Informáticos

Todo medio informático reutilizable de terceros como equipos rentados, discos externos, memorias USB, etc. utilizados por Confecámaras, antes de su entrega se les realizará un proceso de borrado seguro en la información.

7.6.9. Eliminación segura de la información en medios físicos

Cualquier documento físico que haya sido considerado y clasificado de carácter confidencial y que necesite ser destruido, debe realizarse en la respectiva máquina destruye papel.

3.7.7. POLÍTICAS DEL USO DE INTERNET Y CORREO ELECTRÓNICO

3.7.7.1. Prohibición de uso de Internet para propósitos personales.

El uso de Internet está limitado exclusivamente para propósitos laborales. Los usuarios de Internet deben ser advertidos sobre la existencia de recursos tecnológicos que generan registros sobre las actividades realizadas. Esta política se complementa con la política “Instrucciones para el uso de recursos informáticos”.

3.7.7.2. Formalidad del correo electrónico.

Toda comunicación a través del correo electrónico interno se considera una comunicación de tipo laboral y formal, por tanto podrá ser supervisada por el superior inmediato del empleado.

3.7.7.3. Preferencia por el uso del correo electrónico.

Debe preferirse el uso del correo electrónico al envío de documentos físicos siempre que las circunstancias lo permitan.
7.7.4. Uso de correo electrónico.

La cuenta de correo asignada es de carácter individual por lo cual ningún empleado bajo ninguna circunstancia debe usar la cuenta de otro empleado.

3.7.7.5. Revisión del correo electrónico.

Todos los usuarios que dispongan de correo electrónico están en la obligación de revisarlo al menos tres veces diarias. Así mismo, es su responsabilidad mantener espacio libre en el buzón.

3.7.7.6. Mensajes prohibidos.

Se prohíbe el uso del correo electrónico con fines religiosos, políticos, lúdicos o personales o en beneficio de terceros ó que vulnere los derechos fundamentales de las personas. Por tanto, está prohibido el envío, reenvío o en general cualquier otra conducta tendiente a la transmisión de mensajes humorísticos, pornográficos, en cadena, publicitarios y en general cualquier otro mensaje ajeno a los fines laborales sin importar si son de solo texto, audio, video o una combinación de los tres.

3.7.7.7. Acciones para frenar el SPAM.

En el caso de recibir un correo no deseado y no solicitado (también conocido como SPAM), el usuario debe abstenerse de abrirlo y avisar inmediatamente al área de sistemas.

3.7.7.8. Todo buzón de correo debe tener un responsable.

Todo buzón de correo asignado debe tener una persona responsable de su administración, incluidos los buzones de las aplicaciones.

3.7.7.9. Enviando software e información sensible a través de Internet.

Software e información sensible de Confecámaras que requiera ser enviado por Internet debe transmitirse con la mayor seguridad posible acordada entre las partes.

3.7.7.10. Intercambio de información a través de Internet.

La información interna puede ser intercambiada a través de Internet pero exclusivamente para propósitos laborales, con la debida aprobación y usando los mecanismos de seguridad apropiados.

3.7.8. POLÍTICAS DE LA INTRANET Y SITIOS WEB DE CONFECÁMARAS

3.7.8.1. Reglas de uso de la Intranet.

Confecámaras utiliza la intranet como un recurso de publicación de los documentos que rigen la relación entre ésta y el empleado o trabajador. Por lo tanto, el empleado debe consultar la intranet permanentemente, así como todos los documentos que en ella se encuentran publicados.

3.7.8.2. Prohibición de publicitar la imagen de Confecámaras en sitios diferentes a los institucionales.

La publicación de logos, marcas o cualquier tipo de información sobre Confecámaras o sus actividades en Internet solo podrá ser realizada a través de las páginas institucionales de la misma y previa autorización de la Presidencia Ejecutiva. En consecuencia, se encuentra terminantemente prohibido el manejo de esta información en páginas personales de los empleados.

3.7.8.3. Prohibición establecer conexiones a los sitios Web de Confecámaras

Está prohibido igualmente establecer enlaces o cualquier otro tipo de conexión a cualquiera de los sitios Web de Confecámaras por parte de los empleados y de sus sitios Web o páginas particulares, salvo previa autorización de la Presidencia, dependiendo del caso. Particularmente se encuentra prohibido el establecimiento de links o marcos electrónicos, y la utilización de nombres comerciales o marcas de propiedad de la Entidad en sitios diferentes a los institucionales o como meta-etiquetas.

3.7.8.4. Prohibición de anuncios en sitios Web particulares.

Está terminantemente prohibido anunciarse en los sitios Web particulares como empleados de Confecámaras o como sus representantes, o incluir dibujos o crear diseños en los mismos que lleven al visitante del sitio Web a pensar que existe algún vínculo con Confecámaras

3.7.9. POLÍTICAS GENERALES DE LA PRESIDENCIA

3.7.9.1. Evaluación y tratamiento del riesgo

La evaluación de riesgos debería identificar, cuantificar y priorizar los riesgos frente a los criterios de aceptación del riesgo y los objetivos pertinentes para la organización. Los resultados deberían guiar y determinar la acción de gestión adecuada y las prioridades tanto para la gestión de los riesgos de seguridad de la información como para implementar los controles seleccionados para la protección contra estos riesgos.

El alcance de la evaluación de riesgos puede abarcar a toda la organización, partes de la organización, un sistema individual de información, componentes específicos del sistema o servicios, cuando es factible, realista y útil.

Se debe realizar una evaluación de riesgos a los recursos informáticos de Confecámaras por lo menos una vez al año utilizando el procedimiento Interno: “Análisis de riesgos”

3.7.9.2. Restricción por acceso telefónico e Internet sobre recursos tecnológicos de uso interno a clientes externos.

No se otorgarán privilegios de acceso telefónico o Internet a terceros a no ser que la necesidad de dicho acceso sea justificada y aprobada. En tal caso se deben habilitar privilegios específicos para ese usuario, con vigencia solamente del período de tiempo necesario para la actividad justificada y mediante el uso de los mecanismos de control de acceso aprobados por la Presidencia.

3.7.9.3. Los computadores multiusuario y sistemas de comunicación deben tener controles de acceso físico apropiados.

Todos los computadores multiusuario, equipos de comunicaciones, otros equipos que contengan información sensible y el software licenciado de propiedad de la Entidad deben ubicarse en centros de cómputo con puertas cerradas y controles de acceso físico apropiados.

3.7.9.4. Entrenamiento compartido para labores técnicas críticas.

Al menos dos personas deben tener la misma capacidad técnica para la adecuada administración de los sistemas de información críticos de Confecámaras

3.7.9.5. Preparación y mantenimiento de planes para la recuperación de desastres y para respuesta a emergencias.

Todo sistema o recurso informático debe tener definido un plan de contingencia para la restauración de la operación. Se debe preparar, actualizar y probar periódicamente un plan para la recuperación de desastres que permita que sistemas y computadores críticos puedan estar operativos en la eventualidad de un desastre. De igual forma se debe crear planes de respuesta a emergencia con el fin de que se pueda dar una pronta notificación de problemas y solución a los mismos en la eventualidad de emergencias informáticas. Estos planes de respuesta a emergencias pueden llevar a la formación de un equipo dedicado a esta labor.

3.7.9.6. Personal competente en el Centro de Cómputo para dar pronta solución a problemas.
Con el fin de garantizar la continuidad de los sistemas de información, Confecámaras y las cámaras de comercio deben contar con personal técnico competente que pueda detectar problemas y buscar la solución de una forma eficiente.

3.7.9.7. Chequeo de virus en archivos recibidos en correo electrónico.

Confecámaras y las cámaras de comercio deben procurar y disponer de los medios para que todos los archivos descargados de Internet sean chequeados por un software de detección de virus informático, antes de ser transferidos a los computadores de los usuarios.

3.7.9.8. Contacto con grupos especializados en seguridad informática

El personal involucrado con la seguridad de la información deberá tener contacto con grupos especializados o foros relacionados con la seguridad de la información. Esto con el objetivo de conocer las nuevas medidas en cuanto a seguridad de la información se van presentando.

3.7.10. POLÍTICAS PARA DESARROLLADORES DE SOFTWARE
7.10.1.Ambientes separados de producción y desarrollo.

Todo sistema o aplicativo debe contar con ambiente de desarrollo y ambiente de producción. Así mismo para la realización de pruebas no se deben utilizar datos de producción. El Gerente del RUES es responsable de controlar y verificar el cumplimiento de esta política.

3.7.10.2.Cumplimiento del procedimiento para cambios y/o actualizaciones.

Todo cambio y/o actualización en los sistemas de información que se encuentren en producción, serán evaluadas en ambientes de prueba cuya función es determinar el correcto funcionamiento y compatibilidad con las herramientas base. Una vez determinado el correcto funcionamiento y compatibilidad con las herramientas base se debe crear un plan de trabajo para la migración del ambiente de producción a la nueva versión.

3.7.10.3.Documentación de cambios y/o actualizaciones.

Todo cambio y/o actualización en los sistemas de información que se encuentren en producción, debe tener la documentación respectiva.

3.7.10.4.Catalogación de programas.

Debe cumplirse con el procedimiento establecido para pasar programas del ambiente de desarrollo al ambiente de producción previa prueba por parte del área encargada.

3.7.10.5.Medidas de seguridad deben ser implantadas y probadas antes de entrar en operación.

Todos los controles de seguridad para los sistemas de información deben ser implantados y probados sobre ambientes de pruebas o desarrollo y antes que dicho sistema entre en operación.

3.7.10.6.Dependencia de la autenticación de usuario en el sistema operativo.

Los desarrolladores de aplicaciones no deberán crear su propio sistema de control de acceso a la aplicación en desarrollo, esta labor deberá recaer en el sistema operativo o en un sistema de control de acceso que mejora las capacidades del sistema operativo. Esta política debe empezar a cumplirse desde la liberación de este documento.

3.7.10.7.Incorporación de contraseñas en el software.

Ninguna contraseña deberá ser incorporada en el código de un software desarrollado o modificado por Confecámaras o sus proveedores, para permitir que las contraseñas sean cambiadas con la regularidad establecida en la política "Cambios periódicos de contraseñas".

3.7.10.8.Acceso del usuario a los comandos del sistema operativo.

Después de haber iniciado una sesión, el usuario debe mantenerse en menús que muestren solo las opciones habilitadas para dicho usuario y de esta manera impedir la ejecución de comandos del sistema operativo y la divulgación de las capacidades del sistema.

3.7.10.9.Se requieren registros de auditoria en sistemas que manejan información sensible.

Todo sistema que maneje información sensible para Confecámaras y las cámaras de comercio debe generar registros de auditoria que guarden toda modificación, adición y eliminación de dicha información.

3.7.10.10. Registros para los usuarios privilegiados en los sistemas en producción que lo permitan.

Toda actividad realizada en los sistemas por usuarios con privilegios de administración debe ser registrada, si los mismos lo permiten, o de lo contrario debe existir un procedimiento alterno de control.

3.7.10.11.Los registros del sistema deben incluir eventos relevantes para la seguridad.

Los sistemas de computación que manejan información sensible deben registrar todos los eventos de seguridad relevantes. Ejemplos de eventos de seguridad

relevantes son: intentos de adivinación de contraseñas, intentos de uso de privilegios no otorgados, modificaciones a la aplicación y modificaciones al sistema.

3.7.10.12.Resistencia de los registros contra desactivación, modificación y eliminación.

Los mecanismos para detectar y registrar eventos de seguridad informática significativos deben ser resistentes a ataques, en los sistemas que permitan dicha configuración. Estos ataques incluyen intentos por desactivar, modificar o eliminar el software de registro y/o los registros mismos.

3.7.10.13. Procesos controlados para la modificación de información del negocio en producción.

La modificación de información en producción debe darse únicamente mediante procesos con privilegios dentro de la aplicación que maneja dicha información. Esto con el fin de evitar que la información pueda ser modificada por medios diferentes a los canales establecidos. Se excluyen los casos de emergencia, previa autorización de la Presidencia.
3.
7.10.14. Validación de entradas en los desarrollos.

El desarrollador debe tener en cuenta durante la elaboración de la aplicación, la validación de las entradas de código con el objeto de evitar la ejecución de comandos que pongan en riesgo la seguridad de los sistemas.

3.7.10.15. Diseño de seguridad para aplicaciones.

El esquema de seguridad de aplicación, debe elaborarse de acuerdo con las definiciones establecidas para Confecámaras

3.7.10.16. Personas autorizadas para leer los registros de auditoria.

Los registros de sistemas y aplicaciones no deben estar disponibles para personal no autorizado. Personal no autorizado es aquel que no pertenece a auditoria interna, personal de seguridad informática, personal de administración de sistemas o administradores de bases de datos.

3.7.10.17. Archivo histórico de contraseñas.

En todo sistema multiusuario, software del sistema o software desarrollado localmente se debe mantener un archivo histórico encriptado de las contraseñas anteriores. Este archivo deberá ser usado para prevenir que un usuario seleccione una contraseña ya usada (ver política “Las contraseñas creadas por

usuarios no deben ser reutilizadas") y debe contener como mínimo las últimas cinco (5) contraseñas de cada usuario.

3.7.11. POLÍTICAS PARA ADMINISTRADORES DE SISTEMAS
3.7.11.1. Soporte para usuarios con privilegios especiales.

Todos los sistemas y computadores multiusuarios deben soportar un usuario con privilegios superiores a un usuario normal con el fin de poder ejercer las correspondientes labores administrativas y por lo cual estos privilegios deben ser asignados únicamente a los administradores.

3.7.11.2. Los privilegios de acceso a los sistemas de información otorgados a un usuario terminan cuando el usuario finaliza su vínculo contractual con la Entidad.

Todos los privilegios sobre los recursos informáticos de Confecámaras otorgados a un usuario deben eliminarse en el momento que éste abandone la Entidad y la información almacenada queda en manos de su jefe inmediato para aplicar los procedimientos de retención o destrucción de información.

3.7.11.3. Cuando y como pueden asignar contraseñas los administradores

Las contraseñas iniciales otorgadas por el administrador deben servir únicamente para el primer ingreso del usuario al sistema. En ese momento el sistema debe obligar al usuario a cambiar su contraseña.

3.7.11.4. Límite de intentos consecutivos de ingreso al sistema.

El sistema debe limitar el número de intentos consecutivos de introducir una contraseña valida. Después de tres (3) intentos el usuario debe pasar a alguno de los siguientes estados: a) ser suspendido hasta nueva reactivación por parte del administrador; b) ser temporalmente bloqueado (no menos de 5 minutos); c) ser desconectado si se trata de una conexión telefónica.

3.7.11.5. Cambio de contraseñas por defecto.

Todas las contraseñas por defecto que incluyen equipos y sistemas nuevos deberán ser cambiadas antes de su utilización siguiendo los lineamientos de la política "Contraseñas fuertes".

3.7.11.6. Cambio de contraseñas después de compromiso detectado en un sistema multiusuario.

Si un sistema multiusuario utiliza contraseñas como su sistema de control de acceso principal, el administrador del sistema debe asegurarse de que todas las contraseñas del mismo sean cambiadas de forma inmediata si se conoce

evidencia de que el sistema ha sido comprometido. En este caso los usuarios deben ser advertidos de cambiar su contraseña en otros sistemas en los que estuvieran utilizando la misma contraseña del sistema en cuestión.

3.7.11.7. Administración de los buzones de correo.

Los administradores deben establecer y mantener un proceso sistemático para la creación y mantenimiento de los buzones de correo electrónico, mensualmente se realizará una revisión de control sobre cada uno de los buzones creados para determinar cuáles requieren una depuración para que no alcancen su límite de espacio asignado.

3.7.11.8. Brindar acceso a personal externo.

El ingeniero de soporte y web master velará porque individuos que no sean empleados, contratistas o consultores de Confecámaras no tengan privilegio alguno sobre los recursos tecnológicos de uso interno de la Entidad a menos que exista una aprobación escrita de la Presidencia o el comité de seguridad.

3.7.11.9. Acceso a terceros a los sistemas de la Entidad requiere de un contrato firmado.

Antes de otorgarle acceso a un tercero a los recursos tecnológicos de Confecámaras se requiere la firma de un formato, acuerdo o autorización de la Presidencia. Es obligatoria la firma del acuerdo de confidencialidad.

3.7.11.10. Restricción de administración remota a través de Internet.

La administración remota desde Internet no es permitida a menos que se utilicen mecanismos para encripción del canal de comunicaciones.

3.7.11.11. Dos usuarios requeridos para todos los administradores.

Administradores de sistemas multiusuarios deben tener dos identificaciones de usuario: una con privilegios de administración y otra con privilegios de usuario normal.

3.7.11.12. Privilegios por defecto de usuarios y necesidad de aprobación explícita por escrito.

Sin autorización escrita de la Gerencia de Servicios Camerales o la Dirección de TI de las cámaras de comercio, los administradores no deben otorgarle privilegios de administración a ningún usuario.

3.7.11.13. Negación por defecto de privilegios de control de acceso a sistemas cuyo funcionamiento no es apropiado.

Si un sistema de control de acceso no está funcionando adecuadamente, el administrador debe negar todo intento de acceso hasta que su operación normal se haya recuperado.

3.7.11.14. Remoción de software para la detección de vulnerabilidades cuando no esté en uso.

Las herramientas de detección de vulnerabilidades usadas por los administradores se deben desinstalar cuando no estén operativas o implementar un mecanismo de control de acceso especial basado en contraseñas o en encripción del software como tal.

3.7.11.15. Manejo administrativo de seguridad para todos los componentes de la red.

Los parámetros de configuración de todos los dispositivos conectados a la red de Confecámaras deben cumplir con las políticas y estándares internos de seguridad.

3.7.11.16. Información a capturar cuando un crimen informático o abuso es sospechado.

Para suministrar evidencia para investigación, persecución y acciones disciplinarias, cierta información debe ser capturada inmediatamente cuando se sospecha un crimen informático o abuso. Esta información se deberá almacenar de forma segura en algún dispositivo fuera de línea. La información a recolectar incluye configuración actual del sistema, copias de backup y todos los archivos potencialmente involucrados.

3.7.11.17. Sincronización de relojes para un registro exacto de eventos en la red.

Los dispositivos multiusuario conectados a la red interna de Confecámaras deben tener sus relojes sincronizados con la hora oficial.

3.7.11.18. Revisión regular de los registros del sistema.

El área de sistemas debe revisar regularmente los registros de cada uno de los diferentes sistemas para tomar acción oportuna sobre los eventos relevantes de seguridad informática.

3.7.11.19. Confidencialidad en la información relacionada con investigaciones internas.

Hasta que no se hayan presentado cargos o se haya tomado alguna acción disciplinaria, toda investigación relacionada con abusos de los recursos tecnológicos o actividad criminal debe ser confidencial para mantener la reputación del empleado.

3.7.11.20. Información con múltiples niveles de clasificación en un mismo sistema.

Si un sistema o computador maneja información con diferentes niveles de sensibilidad, los controles usados deben ser los adecuados para proteger la información más sensible.

3.7.11.21. Segmentación de recursos informáticos por prioridad de recuperación.

Se debe establecer y usar un marco lógico para la segmentación de recursos informáticos por prioridad de recuperación. Esto hará que los sistemas más críticos sean recuperados primero. Todos los departamentos deberán usar el mismo marco para preparar los planes de contingencia a los sistemas de información.

3.7.11.22. Software de identificación de vulnerabilidades.

Para asegurar que el equipo técnico de Confecámaras y las cámaras de comercio han tomado las medidas preventivas adecuadas, a todos los sistemas conectados a Internet se les debe correr un software de identificación de vulnerabilidades por lo menos una vez al año; adicionalmente en las estaciones de trabajo se cuenta con un software de Cortafuegos y Antivirus que cuente con una consola de administración en la cual se visualizan los reportes de eventos relacionados con vulnerabilidades. A nivel Corporativo se cuenta con un firewall que proporciona un software de IDS (Instrusion Detection System), detección de virus y bloqueo de correo no deseado.

3.7.11.23. En dónde usar controles de acceso para sistemas informáticos.

Todo computador que almacene información sensible de Confecámaras y las cámaras de comercio, debe tener un sistema de control de acceso para garantizar que esta información no sea modificada, borrada o divulgada.

3.7.11.24. Mantenimiento preventivo en computadores, sistemas de comunicación y sistemas de condiciones ambientales

Se debe realizar mantenimiento preventivo regularmente en todos los computadores y sistemas para que el riesgo de falla se mantenga en un nivel bajo.

7.11.25.Habilitación de Logs en Sistemas y Aplicaciones

Se debe habilitar la gestión de logs (archivos de transacción) en los sistemas y aplicaciones críticas de Confecámaras

3.7.11.26.Monitoreo de Sistemas

Se debe mantener una adecuada aplicación de monitoreo configurada que identifique el mal funcionamiento de los sistemas controlados.

3.7.11.27.Mantenimiento de los Sistemas

Se debe realizar periódicamente el mantenimiento en las bases de datos, antivirus, servidores de correo y servicios de Confecámaras

3.7.11.28.Verificación física de equipos críticos

Se debe verificar periódicamente el estado físico de los equipos de cómputo críticos.

3.7.11.29.Servicios de Red

Se debe garantizar que el servicio de red utilizado por Confecámaras y las cámaras de comercio se encuentre disponible y operando adecuadamente, el administrador del sistema o una persona autorizada por el comité de seguridad puede efectuar escaneos de la red con la finalidad de: resolver problemas de servicio, como parte de las operaciones normales del sistema y del mantenimiento, para mejorar la seguridad de los sistemas o para investigar incidentes de seguridad.

3.7.11.30.Revisión de accesos de usuarios

Se debe realizar por control de auditoría la revisión de los accesos de los usuarios a las aplicaciones utilizadas, por lo menos dos veces por año.

3.7.12. POLÍTICAS DE BACKUP
3.7.12.1.Período de almacenamiento de registros de auditoria.

Registros de aplicación que contengan eventos relevantes de seguridad deben ser almacenados por un período no menor a tres (3) meses. Durante este período los registros deben ser asegurados para evitar modificaciones y para que puedan ser vistos solo por personal autorizado. Estos registros son importantes para la corrección de errores, auditoría forense, investigaciones sobre fallas u omisiones de seguridad y demás esfuerzos relacionados.
3.
7.12.2.Tipo de datos a los que se les debe hacer backup y con qué frecuencia.

A toda información sensible y software crítico de Confecámaras residente en los recursos informáticos, se le debe hacer backup con la frecuencia necesaria soportada por el procedimiento de copias de respaldo. Se deben hacer pruebas periódicas para garantizar el buen estado de la información almacenada.

3.7.12.3.Copias de información sensible.

Se deben elaborar una copia de cada backup con el fin de minimizar el riesgo por daño del medio de almacenamiento en disco y cinta, según procedimiento de copias de respaldo.

3.7.13. POLÍTICAS DE USO DE FIREWALL

3.7.13.1.Detección de intrusos.

Todo segmento de red accesible desde Internet debe tener un sistema de detección de intrusos (IDS) con el fin de tomar acción oportuna frente a ataques.

3.7.13.2.Toda conexión externa debe estar protegida por el firewall.

Toda conexión a los servidores de Confecámaras proveniente del exterior, sea Internet, acceso telefónico o redes externas debe pasar primero por el Firewall. Esto con el fin de limitar y controlar las puertas de entrada a la organización.

7.13.3.Toda conexión hacia Internet debe pasar por el Firewall.

El firewall debe ser el único elemento conectado directamente a Internet por lo cual toda conexión desde la red interna hacia Internet debe pasar por el firewall.

3.7.13.4.Filtrado de contenido activo en el Proxy.

La Gerencia de Servicios Camerales de Confecámaras y la direcciones de TI de las cámaras de comercio, deben asegurar que dentro de las definiciones de políticas de Proxy, se filtre todo contenido activo como applets de java, adobe flash player, controles de ActiveX debido a que estos tipos de datos pueden comprometer la seguridad de los sistemas de información de Confecámaras

7.13.5.Firewall debe correr sobre un computador dedicado o appliance.

Todo firewall debe correr sobre un computador dedicado o modelo appliance para estos fines. Por razones de desempeño y seguridad no debe correr otro tipo de aplicaciones.

3.7.13.6.Inventario de conexiones.

Se debe mantener un registro de las conexiones a redes externas con el fin de tener una imagen clara de todos los puntos de entrada a la organización, lo anterior se cumple con el diagrama de red.

3.7.13.7.El sistema interno de direccionamiento de red no debe ser público.

Las direcciones internas de red y configuraciones internas deben estar restringidas de tal forma que sistemas y usuarios que no pertenezcan a la red interna no puedan acceder a esta información.
7.13.8.Revisión periódica y reautorización de privilegios de usuarios.

Los privilegios otorgados a un usuario deben ser reevaluados una vez al año con el fin de analizar sí los privilegios actuales siguen siendo necesarios para las labores normales del usuario, o si se necesita otorgarle privilegios adicionales. Esta política debe ser ejecutada por el área de sistemas con la participación de cada uno de los jefes de área, quienes harán la revisión y solicitud de cambios a la Presidencia.

3.7.14. POLÍTICAS PARA USUARIOS EXTERNOS

7.14.1.Términos y condiciones para clientes de Internet.

Confecámaras y las cámaras de comercio asumen que todos los clientes que usan Internet para establecer relación con Confecámaras o realizar operaciones con las cámaras de comercio aceptan los términos y condiciones impuestos por Confecámaras y las cámaras de comercio en sus términos y condiciones de uso del portal de internet, antes de realizarse cualquier transacción.
3.7.14.2.Acuerdos con terceros que manejan información o cualquier recurso informático de Confecámaras

Todos los acuerdos relacionados con el manejo de información o de recursos de informática de Confecámaras por parte de terceros, deben incluir una cláusula especial que involucre confidencialidad y derechos reservados. Esta cláusula debe permitirle a Confecámaras ejercer auditoría sobre los controles usados para el manejo de la información y específicamente de cómo será protegida la información de Confecámaras

3.7.14.3.Definición clara de las responsabilidades de seguridad informática de terceros.

Socios de negocios, proveedores, clientes y otros asociados a los negocios de Confecámaras deben tener conocimiento de sus responsabilidades relacionadas con la seguridad informática y esta responsabilidad se debe ver reflejada en los contratos con Confecámaras y verificada por la Presidencia, el responsable del manejo de estos terceros deberá realizar un acompañamiento controlado durante

su estadía en las instalaciones de Confecámaras, y de esta manera podrá verificar la calidad en la entrega de los servicios contratados.

3.7.15. POLÍTICAS DE ACCESO FÍSICO
7.15.1.Reporte de pérdida o robo de identificación.

Todo empleado debe reportar con la mayor brevedad, cualquier sospecha de pérdida o robo de carnés de identificación y tarjetas de acceso físico a las instalaciones.

3.7.15.2.Orden de salida para equipos electrónicos.
Ningún equipo electrónico podrá salir de las instalaciones de Confecámaras sin una orden de salida otorgada por el personal adecuado o sin haber sido registrado en el momento de su ingreso.

3.7.15.3.Orden de salida de activos
Todos los activos que afecten la seguridad de la información de Confecámaras como medios de almacenamiento, CD, DVD, entre otros, y que necesiten ser retirados de la entidad, se debe realizar la autorización de salida por medio del formato de Autorización de salida de activos dispuesto para estos casos.

3.7.15.4.Cuando se da una terminación laboral, los privilegios de acceso a la sede de Confecámaras deben ser revocados.

Cuando exista una terminación laboral, el usuario deberá devolver los objetos de acceso físico a las instalaciones (carnés, tarjetas de acceso, etc.) y a su vez todos sus privilegios de acceso deberán ser revocados enviando (funcionarios autorizados) correo electrónico al área de Sistemas (directorit@confecamaras.org.co)

3.7.15.5. Ingreso de equipos de grabación y fotografías al Cuarto de servidores
Cualquier miembro de Confecámaras y/o tercero debe estar autorizado por el área de seguridad de la información para ingresar con equipos donde puedan obtener información, estos pueden ser (video cámaras, celulares, cámaras fotográficas etc.).
8. POLÍTICA DE USO DE PORTÁTILES
8.1. Protección de la información
8.1.1. El antivirus siempre debe estar activo y actualizado
8.1.2. No permitir que personas extrañas lo observen mientras trabaja en el equipo portátil, especialmente si esta fuera de las instalaciones de Confecámaras
3.8.1.3. Seguir las políticas de acceso remoto
3.8.1.4. Toda la información que es confidencial debe ir cifrada.
3.8.1.6. Cuando el equipo deba ser devuelto a Confecámaras para reparación, mantenimiento etc. La información confidencial deberá ser borrada y respectivamente guardada en una copia de respaldo

3.8.1.7. De la información de usuario debe generarse copia de respaldo, por solicitud del usuario al área de sistemas

3.8.2. Protección del equipo portátil
3.8.2.1. No dejar el computador móvil en lugares públicos
3.8.2.2. Cuando viaje el computador portátil no debe ir dentro de su maletero 3.siempre debe llevarse en su mano.
8.2.3. Cuando vaya en su carro este debe ir en el baúl.
3.8.2.4. No prestar el computador portátil a familiares y/o amigos

3.9. ACTUALIZACIÓN, MANTENIMIENTO Y DIVULGACIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.

Éste documento se debe revisar a intervalos planificados o cuando se produzcan cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz.

El Jefe de Riesgos debe aprobar el documento, es responsable por su publicación y comunicación a todos los empleados y partes externas pertinentes. El mecanismo de notificación y divulgación de los cambios realizados a la política de seguridad de la información será mediante correo electrónico.

3.10. COMITÉ DE SEGURIDAD

El Comité de Seguridad de la información está conformado por un equipo de trabajo interdisciplinario encargado de garantizar una dirección clara y brindar apoyo visible a la Presidencia con respecto al programa de seguridad de la información dentro de la organización.

El comité debe estar a cargo de promover la seguridad de la organización por medio de un compromiso apropiado y contar con los recursos adecuados.

Las siguientes son las principales responsabilidades a cargo del Comité de Seguridad De la información, dentro de la Entidad:

- Revisión y seguimiento al modelo de gobierno de seguridad de la información a implementar en la organización.
- Revisión y valoración de la Política de Seguridad de la Información.
- Alineación e integración de la seguridad a los objetivos del negocio.
- Garantizar que la seguridad de la información forma parte integral del proceso de planeación estratégica de la organización.

- Establecer las funciones y responsabilidades específicas de seguridad de la información para toda la compañía.
- Reportar, a través de reuniones semestrales a la Presidencia el estado de la seguridad y protección de la información en la compañía y la necesidad de nuevos proyectos en temas de seguridad de la información
- Establecer y respaldar los programas de concientización de la compañía en materia de seguridad y protección de la información
- Establecer, evaluar y aprobar el presupuesto designado para el tema de seguridad de la información
- Evalúa la adecuación y coordina la implementación de los controles de seguridad específicos para nuevos servicios o sistemas de información.
- Promueve explícitamente el apoyo institucional a la seguridad de la información en toda la organización.
- Supervisión y control de los cambios significativos en la exposición de los activos de información a las principales amenazas.
- Revisión y seguimiento a los incidentes de seguridad de la información.
- Analizar y autorizar cualquier tipo de movimiento o traslado de equipos de misión crítica para la compañía.

Adicionalmente, el comité tiene la responsabilidad de tratar los siguientes temas (por demanda):

- Mejoras en las actividades inherentes a la Seguridad de Confecámaras y sus procesos.
- Seguimiento a la aplicación de las políticas, programas y planes adoptados para la protección de los sistemas, recursos informáticos y servidores de la Red Interna y Centro de Cómputo de Confecámaras
- Decisiones de carácter preventivo y proactivo que apunten a la optimización de la seguridad de los procesos y sus procedimientos.

- Cambio en los roles del ciclo de certificación.
- Participación activa en la revisión, evaluación, mantenimiento, recomendaciones, mejoras y actualizaciones de la presente política de Confecámaras El Presidente Convoca al comité de seguridad con el propósito de evaluar los cambios a la presente política y autorizar su publicación. De este comité se deja Acta como constancia de su evaluación y aprobación.

  - Las decisiones del comité de seguridad son protocolizadas mediante un Acta de Comité de Seguridad firmada por los miembros, así:
  - Vicepresidente Ejecutivo
  - Gerente RUES
  - Gerente de Servicios Camerales
  - Director de Desarrollo

- Jefe de Servicios Tecnológicos

Las Actas de comité de seguridad podrán ser Anuladas por el comité de Seguridad mediante el uso de un Acta que invalide el contenido siempre y cuando no se haya(n) ejecutado la(s) acción(es) relacionadas.

3.10.1. Oficial de Seguridad de la Información

Oficial de Seguridad de la Información (Jefe de Riesgos):

- Identificar y satisfacer las necesidades de capacitación en temas de seguridad de la información a los funcionarios de la compañía.
- Actualización y seguimiento periódico al mapa de riesgos de la compañía, validando con cada proyecto que se implemente como afecta el mapa de riesgos y tomando siempre como base este mapa para cualquier proyecto nuevo que se implemente.
- Dirigir el programa de manejo y seguimiento de incidentes.
- Crear y establecer una metodología de clasificación de la información según su importancia e impacto dentro de la compañía. Igualmente debe informarla a la compañía y validar que se cumpla. La metodología debe establecer niveles de acceso a la información.
- Crear y mantener un Programa de Concientización en seguridad de la información.
- Evaluar en forma continua la efectividad de la seguridad de la información de la organización con el propósito de identificar oportunidades de mejoramiento y necesidades de capacitación

4. PLAN DE TRATAMIENTO DEL RIESGO

4.1 METODOLOGÍA DE ANÁLISIS

El proceso del análisis de riesgos comprende numerosas etapas que develan de una manera u otra la realidad en seguridad de una empresa y la rigurosidad con que la misma esta implementada. La metodología MAGERIT en su versión 3 ha resultado ser un instrumento de amplia difusión y se encontró que para empresas de la misma misión de Confecámaras presentó informes que dieron valor agregado en su momento. Otros aspectos que se resaltan de la metodología de análisis de riesgos seleccionada, son los siguientes:

- La metodología para su implementación esta definida y los documentos que retroalimentan el proceso son claros y de amplia difusión, lo que permite realizar integración o migración a otros estándares de igual forma internacionales.
- El acercamiento de la norma en el idioma español, asegura que el soporte para la misma como sus documentos de ayuda estarán asequibles en todo momento.
- Su metodología de inspección muestra todos los apartes del sistema y su interoperabilidad con los objetivos de la empresa.
- Provee un acercamiento óptimo a todos los términos de la familia de normas ISO enfocados en seguridad.
- Cobija de manera estructurada el objetivo primordial de establecer medidas de seguridad y al mismo tiempo el análisis de riesgos y su respectivo tratamiento.
- De acuerdo a lo anterior Magerit presentó un alineamiento con los objetivos estratégicos de la Confederación colombiana de cámaras de comercio en lo concerniente a su afán por generar un valor agregado incluso desde sus herramientas de análisis y verificación y en particular con los elementos que son producto de análisis dentro del presente Sistema de Gestión de Seguridad de la Información:
- Activos: Son la materia prima de todos los demás recursos que utilizan los datos de la empresa para convertirse en información y pasar a proveer valor a las actividades de la organización.
- Amenazas: Se define como todas las posibles alteraciones o hechos que están en la posibilidad de materializarse y generar algún tipo de afectación.
- Vulnerabilidades: Debilidad propia de un activo que puede generar la repentina repercusión de afectación sobre unos de los pilares de la información.
- Impacto: Aspectos que se generan como producto de la materialización de una amenaza y que son directamente proporcionales al valor propio del activo.
- Riesgo: Es la capacidad innata de que una amenaza, dada su probabilidad, se materialice y repercuta la organización.
- Salvaguardas: Control propio generado a partir del análisis de seguridad y que provee una disminución en la posibilidad de ocurrencia en lo que respecta a las amenazas.

Magerit en el análisis de riesgos desde sus aspectos sistémicos, acerca la determinación del riesgo, siguiendo una seria de etapas:

- 1: Inventario de Activos
- 2: Valoración de los activos
- 3: Amenazas (incluidas la identificación y la valoración)
- 4: Salvaguardas

- 5: Informe sobre la evaluación de riesgos
- 6: Resultados del análisis de riesgos

4.3GESTIÓN DEL RIESGO

Una vez se ha detectado la posibilidad de ocurrencia de un evento, que ponga en riesgo la integridad, disponibilidad o confiabilidad de la información, en Confecámaras se iniciará un ciclo de análisis de la situación que está definido por Magerit en su versión número tres.

Las etapas podrán tener un ciclo de análisis continuo y el mismo se abandonará siempre y cuando la amenaza residual pueda ser asumida o descartada.

Respecto a los resultados del análisis de riesgos, se determinó por parte del comité de seguridad, que las amenazas que serán atendidas de manera inmediata, serán las caracterizadas como: Altas y Muy Altas.

Para las amenazas dentro del rango Medio, se realizarán tareas de monitoreo exhaustivo y en cada reunión del comité se evidenciará el comportamiento de dicha amenaza y se establecerá un nuevo nivel de riesgo para la misma.

Dado que el proceso de gestión del riesgo y en particular para situaciones que deriven en análisis forenses, amenazas tipo “Día 0”, o ataques inminentes, se establecerán ciertas etapas, dentro de las cuales es necesario determinar que o cuales figuras dentro del marco operativo entrarán en juego para las decisiones respectivas. Dichas personas o el responsable actual del cargo equivalente, estarán en la obligación de retroalimentar en cada momento la situación generando una operatividad continua de comunicación y consulta además de seguimiento y control a todos los demás integrantes del comité de seguridad, establecido en el documento de continuidad del negocio.

En la primera etapa denominada “Determinación del contexto”, cualquiera de los integrantes del comité analizará la situación potencial y lo comunicara de inmediato, intentando suministrar la mayor cantidad de información que le sea posible y acudiendo al manual de políticas de seguridad puntualmente al numeral “12.4.1 Registro y gestión de eventos de actividad” y de esta manera proveer elementos de juicio a los demás analistas de la situación.

La apreciación del riesgo enmarcara las siguientes ejecuciones:

- Identificación
- Análisis
- Evaluación

Cada uno de los segmentos deberá ser debatido por cualquier medio que se facilite y en todo caso deberá compartirse la información entre todos los miembros. Una vez entregado el diagnostico, se definirá de manera unánime si es necesario desplegar algún tipo de recurso para su atención y en caso tal se brindara el tratamiento y se operará de acuerdo a la política de seguridad y el resultado será materia de seguimiento y revisión con el fin de determinar cualquier de las siguientes posibilidades en lo referente al riesgo:

Aceptación: Implica un bajo costo en lo referente al cumplimiento de la misión de Confecámaras y esto está ligado al impacto que pueda tener y a la capacidad de recuperación que en términos de tiempo, dinero o prestigio estén en juego.

Mitigación: Es el objetivo de las salvaguardas establecidas en el informe sobre evaluación y tratamiento de riesgos y su aplicación se realizara de manera autónoma por parte del comité de seguridad, siempre y cuando no exista un riesgo residual adicional que pueda comprometer activos o daños colaterales de un impacto considerable, en este caso se agotará la transferencia del mismo.

Transferencia: Procederá cuando haya lugar y la protección en termas contractuales, de garantías, pólizas o seguros pueda ser aplicada. Este recurso deberá estar avalado por el comité de seguridad y todas las partes legales de responsabilidad estén claramente definidas y aprobadas.

Evasión: Aplicará en casos excepcionales en los cuales la ecuación Valor / Servicio sea demasiado baja y descartar el activo sea mucho más beneficioso que aplicar cualquier otro tipo de salvaguardas. Se deja claro que este tipo de tratamiento es el más extremo y el que menos experiencia en el reproceso ofrece.

Cuando se ha establecido que el riesgo y que su ocurrencia son mínimos, en cualquiera de sus alcances, deberá analizarse las salvaguardas que se vieron comprometidas en la gestión de las amenazas y se deberá definir si la misma o mismas deben ser reforzadas de alguna manera puntual. El tema económico es el más comprometido y es necesario tomar decisiones sobre si la operación o el costo de mantenerla con un menor nivel de incertidumbre es asumible por la organización.

4.4INVENTARIO DE ACTIVOS

Como base fundamental del proyecto de Sistema de Gestión de la información en la Confederación Colombiana de Cámaras de comercio, se adelantó en conjunto con las áreas operativas de la entidad, incluyendo a todos los involucrados en gestión de soporte en áreas de comunicación y sistemas, un inventario, tal como se ilustra en la Tabla 1 de Inventario de equipos, que pretendió establecer cuáles

son los activos que tienen un peso significativo y que presentan un nivel de riesgo y cuyas vulnerabilidades, si las tuviesen o si las presentasen, enfrentarían a la entidad a un desastre informático inminente. El modelo que se aplicó para la recolección de la información dimensiono tanto las particularidades del modelo Magerit como la aproximación real al modelo usado por la entidad así como la referencia al interior de la entidad. La tabla No.1 está asociada a la clasificación que presenta Magerit para sus análisis y que permitirá en referencias posteriores un acercamiento asertivo al activo:

Tabla 1: Inventario de activos

INVENTARIO DE ACTIVOS

A. Activos esenciales

CODIGO GRUPO DE ACTIVO MAGERIT	NOMBRE GRUPO DE ACTIVO MAGERIT	CODIGO ACTIVO DE ACUERDO A LA EMPRESA	NOMBRE ACTIVO DE ACUERDO A LA EMPRESA
[vr]	Datos vitales	[I_Clientes_Camaras]	Información de las Cámaras de Comercio
		[I_Aplicativo_SII]	Información de aplicaciones del servicio registral
[classified]	Datos clasificados	[C_F_Aplicaciones]	Código fuente: diseño, planes de pruebas
		[H_CodigoFuente]	Histórico codigo fuente de aplicaciones
		[D_Proyectos]	Documentación de proyectos
		[D_Proyectos_convenios]	Documentación de proyectos Convenios

B. Datos/Información

CODIGO GRUPO DE ACTIVO MAGERIT	NOMBRE GRUPO DE ACTIVO MAGERIT	CODIGO ACTIVO DE ACUERDO A LA EMPRESA	NOMBRE ACTIVO DE ACUERDO A LA EMPRESA
[files]	Ficheros	[F_clientes internos]	Archivos de clientes internos
[conf]	Datos de configuracion	[D_Doc_infraestructura]	Datos de configuracion de servidores y equipos
[int]	Datos de gestión interna	[D_GestionProyectos]	Datos de Gestión de proyectos
[password]	Credenciales	[Pass_usuarios]	Credenciales de acceso tanto para usuarios dentro de la empresa como de forma remota
[acl]	Datos de control de acceso	[Control_acceso_datacenter_Synapsis]	Controles de acceso al CPD.
		[Control_acceso_datacenter_col_XV]	Controles de acceso al CPD.

C. Claves Criptográficas Conectividad para certificados virtuales de las Cámaras de Comercio

CODIGO GRUPO DE ACTIVO MAGERIT	NOMBRE GRUPO DE ACTIVO MAGERIT	CODIGO ACTIVO DE ACUERDO A LA EMPRESA	NOMBRE ACTIVO DE ACUERDO A LA EMPRESA
[encrypt]	Claves de cifra	[CC_plataformas_pagos_electro]	Claves de cifra pagos en linea
[sign]	Llaves de firma	[llaves_p12]	Llaves criptograficas

D. Servicios	Servicios tecnologicos ofrecidos por parte de la Confederacion Colombiana de Camaras de Comercio		
CODIGO GRUPO DE ACTIVO MAGERIT	**NOMBRE GRUPO DE ACTIVO MAGERIT**	**CODIGO ACTIVO DE ACUERDO A LA EMPRESA**	**NOMBRE ACTIVO DE ACUERDO A LA EMPRESA**
[ext]	A usuarios externos (bajo una relación contractual)	[S_U_Externo]	Servicios prestados a las camaras de comercio bajo el modelo de acuerdo tecnologico
[int]	Interno (a usuarios de la propia organización)	[S_U_Interno]	Servicios prestados a los usuarios internos a traves del aplicativo web
[www]	World wide web	[S_Internet]	Servicio de internet ofrecido desde el datacenter
[email]	Correo electrónico	[S_correo]	Servidor de Correo zimbra
		[S_correo_ext]	Servidor de Correo OWA
[file]	Almacenamiento de ficheros	S_A_Bases de datos]	Bases de datos de los aplicativos web
[ipm]	Gestión de privilegios	[G_privilegios]	Nivel de acceso a traves de firewall desde conexiones
[edi]	Intercambio electrónico de datos	[D_D_Electronicamente]	Repositorios FTP del RUES
[idm]	Gestión de identidades	[G_Identidades]	Control de acceso a servicios de pagos electronicos en SIPP
[pki]	PKI - infraestructura de clave pública	[Firmado_p12]	Firmado automatico de certificados de camaras de comercio
	PKI - infraestructura de clave pública	[Conexión_Cifrada_Regist]	Conexión cifrada para la interconectividad protegida con la registraduria general de la nacion

E. Aplicaciones	Los acuerdos tecnologicos celebrados por confecamaras con las caámaras de comercio de colombia establecen entre otras cosas niveles de software como servicio y plataforma tecnologica como servicio:		
CODIGO GRUPO DE ACTIVO MAGERIT	**NOMBRE GRUPO DE ACTIVO MAGERIT**	**CODIGO ACTIVO DE ACUERDO A LA EMPRESA**	**NOMBRE ACTIVO DE ACUERDO A LA EMPRESA**
[prp]	Desarrollo propio (in house)	[Soft_propio]	Software desarrollado por la empresa.
		[Soft_pruebas]	Software en pruebas desarrollado por la empresa
[Sub]	desarrollo a medida (subcontratado)	[Soft_tercerizado]	Acuerdos de software con terceros
[app]	Servidor de aplicaciones	[Server_App_Sirep]	Servidor servicios registrales
		[Server_App_SII]	Servidor web servicios registrales
		[Server_App_RNT]	Servidor Web Registro Nacional de
		[Server_App_CAE]	Servidor Crear empresa
[email_client]	Cliente de correo electrónico	[Cliente_correo]	Outlook para conexión a servidor de correo interno
[email_server]	Servidor de correo electrónico	[Server_correo_zimbra]	Robot SMTP para aplicativos
		[Server_correo_owa]	Servicio de correo empresarial
[dbms]	Sistema de gestión de bases de datos	[DBMS_MySQL]	Navicat Gold
		[DBMS_PostgresSQL]	
		[DBMS_SQLServer]	
		[DBMS_Adabast]	
[os]	Sistema operativo	[SO_Linux]	Sistema Operativo Servidores
		[SO_Windows]	Sistema Operativo funcionarios
		[SO_OSX]	Sistema Operativo Soportes
[hypervisor]	Gestor de máquinas virtuales	[VM_Ware]	Gestor plataforma de virtualización

F. Equipos Informáticos Entran en consideración los equipos informaticos que permiten realizar la operación en Confecámaras.

CODIGO GRUPO DE ACTIVO MAGERIT	NOMBRE GRUPO DE ACTIVO MAGERIT	CODIGO ACTIVO DE ACUERDO A LA EMPRESA	NOMBRE ACTIVO DE ACUERDO A LA EMPRESA
[hosts]	Grandes equipos (Servidor web, Servidor de bases de datos,	[Host_IBM_1]	Host para solucion HA Vmware
		[Host_IBM_2]	
		[Host_IBM_3]	
[mid]	Equipos medios (Equipos de desarrollo conectados a través de red inalámbrica por red 802.1x)	[Server_desa_Amazon]	Servidor de desarrollo en Amazon
		[Server_asterisk]	Servidor telefonia interna
		[Server_correo_owa]	Servidor de Correo OWA
[vhost]	Grandes equipos (Servidor web, Servidor de bases de datos, servidores de aplicación)	[Server_App_Sirep]	Servidor servicios registrales
		[Server_App_SII]	Servidor web servicios registrales
		[Server_App_RNT]	Servidor Web Registro Nacional de Turismo
		[Server_App_CAE]	Servidor Crear empresa
		[Server_MySQL]	Servidor de bases de datos
		[Server_correo_zimbra]	Servidor de Correo zimbra
[router]	Enrutadores	[Router_Level3_Panorama]	Enrutador Red RUES
		[Router_Synapsis]	Enrutador ISP Principal Synapsis
[wap]	Punto de acceso inalámbrico	[Router_Une_Internet]	Acceso internet contingencia
[Firewall]	Cortafuegos	[Juniper_Panrorama]	UTM Panorama
		[Juniper_synapsis]	UTM Datacenter
[switch]	conmutadores	[Sw_panorama_lan]	Switch panorama LAN
	conmutadores	[Sw_panorama_Rues]	Switch panorama red RUES
	conmutadores	[Sw_Synapsis_lan]	Switch Synapsis Lan
[tape]	cinta magnética	[Tape_LTO5	Cintas Magneticas LTO5
[ups]	sistemas de alimentación ininterrumpida	[Ups_Panorama]	Ups Sede Panorama
[robot][tape]	Robot de Cintas	[Ts_2900]	Robot Cintas Datacenter
[san]	almacenamiento en red	[DS_3400]	Almacenamiento 1
		[V3700]	Almacenamiento 2

G. Redes de comunicaciones

CODIGO GRUPO DE ACTIVO MAGERIT	NOMBRE GRUPO DE ACTIVO MAGERIT	CODIGO ACTIVO DE ACUERDO A LA EMPRESA	NOMBRE ACTIVO DE ACUERDO A LA EMPRESA
[wifi]	Red inalámbrica	[Wifi_www]	Wifi contingencia y navegacion libre
[LAN]	Red local	[LAN_corporativa_panorama]	Red corporativa de voz y datos
		[LAN_coporativa_Datacenter_RUES]	Red Datacenter RUES
		[LAN_coporativa_datacenter]	Red LAN Datacenter
[Internet]	Internet	[Wan_coporativa]	Red de internet principal
		[Wan_RUES]	Red de navegacion privada interconexion nacional Camaras

H. Instalaciones

CODIGO GRUPO DE ACTIVO MAGERIT	NOMBRE GRUPO DE ACTIVO MAGERIT	CODIGO ACTIVO DE ACUERDO A LA EMPRESA	NOMBRE ACTIVO DE ACUERDO A LA EMPRESA
[building]	Edificio	[Edif_Panorama]	Edificio panorama principal
		[Edif_Datacenter]	Edificio datacenter ZonaFranca Synapsis

I. Personal

CODIGO GRUPO DE ACTIVO MAGERIT	NOMBRE GRUPO DE ACTIVO MAGERIT	CODIGO ACTIVO DE ACUERDO A LA EMPRESA	NOMBRE ACTIVO DE ACUERDO A LA EMPRESA
[ui]	Usuarios internos	[U_nivel1]	Usuarios de atencion al cliente i E y administrativos de todas las jerarquias
[adm]	Administradores de sistemas	[U_Nivel_3]	Administrador de infraestructura
[des]	Desarrolladores programadores	[U_Nivel_2]	Equipo de desarrollo y soporte

5. EVALUACIÓN Y TRATAMIENTO DE RIESGOS

5.1 VALORACIÓN CUALITATIVA DE LOS ACTIVOS

De acuerdo al modelo de análisis de riesgos de la información: Magerit, los activos deben tener un peso inherente al servicio o al costo que prestan. Esto se mide por el impacto que puede llegar a tener el prescindir de cualquier de estos en el momento en el que se materializa un riesgo.

La Tabla 2, define cuáles serán los criterios usados en el Sistema de Gestión de Seguridad de la información de Confecámaras para la evaluación y tratamiento de Riesgos:

Tabla 2: Valoración de activos

VALORACION DE ACTIVOS - TABLA DE VALORES	
VALOR	**CRITERIO**
10	Daño Muy Grave a la organización
7-9	Daño grave a la organización
4-6	Daño importante a la organización
1-3	Daño menor a la organización
0	Irrelevante para la organizaciçon

6.DIMENSIONAMIENTO CUANTITATIVO DE ACTIVOS

Los valores serán enmarcados apuntando las 5 dimensiones propias de cada activo y las mismas serán calificadas de acuerdo a la medida de daño o impacto para la organización si el activo se ve afectado de en dicha dimensión:
Dimensión Disponibilidad [D]: Se refiere específicamente al impacto que provocaría que un activo no pudiera ser accedido o si el servicio que presta no se pudiera entregar de la manera habitual. Aplica para todo tipo de activo.

Dimensión integridad de los datos [I]: Trata de las consecuencias adversas que para Confecámaras tendría el hecho de que la información que transmite o recibe por parte de sus clientes no pueda ser verificada o que la misma se encuentre seriamente alterada.
Dimensión confidencialidad [C]: Que tanto impacto tendría para la organización que su información sufriera una figa y fuera expuesta públicamente.
Dimensión Autenticidad [A]: Que tan importante seria para la empresa no poder garantizar que quien realiza el uso de un activo sean realmente quien fue inicialmente autorizado para ello.
Dimensión Trazabilidad [T]: Como afectaría a la organización que no pudiera ser identificado el uso de un servicio y a si mismo como podría realizar investigaciones de carácter legal en caso de ser requerido.

Todas las dimensiones conjugadas ofrecen la perspectiva necesario para comprender la importancia de la seguridad tanto en sus subconjuntos como de manera individual. Esta perspectiva es posible de analizarse desde el formato que Magerit exige y que se muestra en la Tabla 3:

Tabla 3: Valoración cualitativa de activos

VALORACION CUALITATIVA DE ACTIVOS									
A. Activos esenciales				DIMENSION / VALOR					
CODIGO GRUPO DE ACTIVO MAGERIT	**NOMBRE GRUPO DE ACTIVO MAGERIT**	**CODIGO ACTIVO DE ACUERDO A LA EMPRESA**	**NOMBRE ACTIVO DE ACUERDO A LA EMPRESA**	**D**	**I**	**C**	**A**	**T**
[vr]	Datos vitales	[I_Clientes_Camaras]	Información de las Cámaras de	10	10	10	10	8
		[I_Aplicativo_SII]	Información de aplicaciones del	9	2	8	4	4
[classified]	Datos clasificados	[C_F_Aplicaciones]	Código fuente: diseño, planes de	8	9	7	4	3
		[H_CodigoFuente]	Histórico codigo fuente de	8	9	7	4	4
		[D_Proyectos]	Documentación de proyectos	8	9	7	4	2
		[D_Proyectos_convenios]	Documentación de proyectos	8	9	7	4	3

B. Datos/Información				DIMENSION / VALOR				
CODIGO GRUPO DE ACTIVO MAGERIT	**NOMBRE GRUPO DE ACTIVO MAGERIT**	**CODIGO ACTIVO DE ACUERDO A LA EMPRESA**	**NOMBRE ACTIVO DE ACUERDO A LA EMPRESA**	**D**	**I**	**C**	**A**	**T**
[files]	Ficheros	[F_clientes internos]	Archivos de clientes internos	8	8	9	9	9
[conf]	Datos de configuracion	[D_Doc_infraestructura]	Datos de configuracion de servidores y equipos	10	9	10	7	5
[int]	Datos de gestión interna	[D_GestionProyectos]	Datos de Gestión de proyectos	8	6	7	8	5
[password]	Credenciales	[Pass_usuarios]	Credenciales de acceso tanto para usuarios dentro de la empresa como de forma remota	10	10	10	8	9
[acl]	Datos de control de acceso	[Control_acceso_datacenter_Synapsis]	Controles de acceso al CPD.	7	6	8	8	5
		[Control_acceso_datacenter_col_XV]	Controles de acceso al CPD.	7	6	8	8	5

C. Claves Criptográficas	Conectividad para certificados virtuales de las Cámaras de Comercio			DIMENSION / VALOR				
CODIGO GRUPO DE ACTIVO MAGERIT	**NOMBRE GRUPO DE ACTIVO MAGERIT**	**CODIGO ACTIVO DE ACUERDO A LA EMPRESA**	**NOMBRE ACTIVO DE ACUERDO A LA EMPRESA**	**D**	**I**	**C**	**A**	**T**
[encrypt]	Claves de cifra	[CC_plataformas_pagos_electro]	Claves de cifra pagos en linea	8	10	10	10	7
[sign]	Llaves de firma	[llaves_p12]	Llaves criptograficas	9	10	10	10	7

D. Servicios			DIMENSION / VALOR				
NOMBRE ACTIVO DE ACUERDO A LA EMPRESA	AMENAZA CLASIFICACON MAGERIT	FRECUENCIA DE LA AMENAZA	D	I	C	A	T
Servicios prestados a las camaras de comercio bajo el modelo de acuerdo tecnologico	[E.2] Errores del administrador	5	75%	75%	100%		
	[A.6] Abuso de privilegios de acceso	5	75%	50%	80%		
Servicios prestados a los usuarios internos a traves del aplicativo web	[E.2] Errores del administrador	5	75%	75%	75%		
	[A.6] Abuso de privilegios de acceso	5	40%	50%	50%		
Servicio de internet ofrecido desde el datacenter	[E.2] Errores del administrador	5	100%	100%	50%		
	[A.6] Abuso de privilegios de acceso	5	50%	50%	90%		
Servidor de Correo zimbra	[E.2] Errores del administrador	5	50%	20%	50%		
	[A.6] Abuso de privilegios de acceso	5	30%	40%	50%		
Servidor de Correo OWA	[E.2] Errores del administrador	5	50%	75%	50%		
	[A.6] Abuso de privilegios de acceso	5	75%	50%	50%		
Bases de datos de los aplicativos web	[E.2] Errores del administrador	5	100%	100%	75%		
	[A.6] Abuso de privilegios de acceso	5	90%	80%	90%		
Nivel de acceso a traves de firewall desde conexiones personales	[E.2] Errores del administrador	5	100%	100%	75%		
	[A.6] Abuso de privilegios de acceso	5	100%	50%	50%		
Repositorios FTP del RUES	[E.2] Errores del administrador	5	20%	50%	50%		
	[A.6] Abuso de privilegios de acceso	5	30%	30%	45%		
Control de acceso a servicios de pagos electronico en SIPP	[E.2] Errores del administrador	5	50%	50%	75%		
	[A.6] Abuso de privilegios de acceso	5	60%	60%	50%		
Firmado automatico de certificados de camaras de comercio	[E.2] Errores del administrador	5	50%	50%	75%		
	[A.6] Abuso de privilegios de acceso	5	70%	95%	50%		
Conexión cifrada para la interconectividad protegida con la registraduria general de la nacion	[E.2] Errores del administrador	5	75%	100%	100%		
	[A.6] Abuso de privilegios de acceso	5	90%	100%	100%		

E. Aplicaciones			DIMENSION / VALOR				
CODIGO GRUPO DE ACTIVO MAGERIT	NOMBRE ACTIVO DE ACUERDO A LA EMPRESA	FRECUENCIA DE LA	D	I	C	A	T
Software desarrollado por la empresa.	[I.5] Avería de origen físico o lógico	10	60%				
	[E.2] Errores del administrador	10	75%	75%	75%		
	[E.20] Vulnerabilidades de los programas (software)	10	50%	50%	50%		
	[A.6] Abuso de privilegios de acceso	3	85%	85%	90%		
Software en pruebas desarrollado por la empresa	[I.5] Avería de origen físico o lógico	10	60%				
	[E.2] Errores del administrador	10	75%	50%	10%		
	[E.20] Vulnerabilidades de los programas (software)		75%	50%	50%		
	[A.6] Abuso de privilegios de acceso	3	85%	70%	90%		
Acuerdos de software con terceros	[I.5] Avería de origen físico o lógico	10	60%				
	[E.2] Errores del administrador	10	75%	75%	75%		
	[E.20] Vulnerabilidades de los programas (software)		75%	50%	50%		
	[A.6] Abuso de privilegios de acceso	3	85%	65%	90%		

NOMBRE ACTIVO DE ACUERDO A LA EMPRESA	AMENAZA CLASIFICACON MAGERIT	FRECUENCIA DE LA AMENAZA	D	I	C	A	T
Servidor servicios registrales	[I.5] Avería de origen físico o lógico	10	60%				
	[E.2] Errores del administrador	5	100%	75%	75%		
	[E.20] Vulnerabilidades de los programas (software)		75%	75%	75%		
	[A.6] Abuso de privilegios de acceso	3	88%	85%	90%		
Servidor web servicios registrales	[I.5] Avería de origen físico o lógico	10	60%				
	[E.2] Errores del administrador	5	100%	75%	100%		
	[E.20] Vulnerabilidades de los programas (software)		75%	50%	50%		
	[A.6] Abuso de privilegios de acceso	3	85%	85%	90%		
Servidor Web Registro Nacional de Turismo	[I.5] Avería de origen físico o lógico	10	60%				
	[E.2] Errores del administrador	5	100%	75%	50%		
	[E.20] Vulnerabilidades de los programas (software)		75%	75%	75%		
	[A.6] Abuso de privilegios de acceso	3	87%	85%	90%		
Servidor Crear empresa	[I.5] Avería de origen físico o lógico	10	60%				
	[E.2] Errores del administrador	5	100%	75%	75%		
	[E.20] Vulnerabilidades de los programas (software)		75%	75%	75%		
	[A.6] Abuso de privilegios de acceso	3	85%	85%	90%		
Outlook para conexión a servidor de correo interno	[I.5] Avería de origen físico o lógico	10	60%				
	[E.9] Errores de [re-]encaminamiento	10	50%				
	[E.2] Errores del administrador	5	5%	50%	75%		
	[E.9] Errores de [re-]encaminamiento	50		75%			
	[E.20] Vulnerabilidades de los programas (software)		20%	50%	50%		
	[A.6] Abuso de privilegios de acceso	3	89%	85%	90%		
Robot SMTP para aplicativos	[I.5] Avería de origen físico o lógico	10	60%				
	[E.9] Errores de [re-]encaminamiento	5	20%				
	[E.2] Errores del administrador	5	50%	50%	75%		
	[E.20] Vulnerabilidades de los programas (software)		30%	40%	40%		
	[A.6] Abuso de privilegios de acceso	3	85%	85%	90%		
Servicio de correo empresarial	[I.5] Avería de origen físico o lógico	10	60%				
	[E.8] Difusión de software dañino	1	20%				
	[E.2] Errores del administrador	5	75%	75%	100%		
	[E.9] Errores de [re-]encaminamiento	50		75%			
	[E.20] Vulnerabilidades de los programas (software)		50%	45%	45%		
	[A.6] Abuso de privilegios de acceso	3	52%	85%	90%		
Navicat Gold	[I.5] Avería de origen físico o lógico	10	60%				
	[E.8] Difusión de software dañino	1	5%				
	[E.2] Errores del administrador	5	5%	20%	50%		
	[E.20] Vulnerabilidades de los programas (software)		5%	10%	20%		
	[A.6] Abuso de privilegios de acceso	3	41%	85%	90%		
Sistema Operativo Servidores	[I.5] Avería de origen físico o lógico	10	60%				
	[E.2] Errores del administrador	5	100%	75%	75%		
	[E.20] Vulnerabilidades de los programas (software)		75%	50%	50%		
	[A.6] Abuso de privilegios de acceso	3	85%	85%	90%		
Sistema Operativo funcionarios	[I.5] Avería de origen físico o lógico	10	60%				
	[E.8] Difusión de software dañino	1	50%				
	[E.2] Errores del administrador	5	75%	50%	50%		
	[E.20] Vulnerabilidades de los programas (software)		75%	50%	50%		
	[A.6] Abuso de privilegios de acceso	3	52%	85%	90%		
Sistema Operativo Soportes	[I.5] Avería de origen físico o lógico	10	60%				
	[E.8] Difusión de software dañino	5	75%				
	[E.2] Errores del administrador	5	75%	75%	50%		
	[E.20] Vulnerabilidades de los programas (software)		75%	50%	50%		
	[A.6] Abuso de privilegios de acceso	3	85%	85%	90%		
Gestor plataforma de virtualización	[I.5] Avería de origen físico o lógico	10	60%				
	[E.2] Errores del administrador	5	100%	50%	50%		
	[E.20] Vulnerabilidades de los programas (software)		100%	75%	75%		
	[A.6] Abuso de privilegios de acceso	3	52%	85%	90%		

F. Equipos Informáticos			DIMENSION / VALOR				
NOMBRE ACTIVO DE ACUERDO A LA EMPRESA	AMENAZA CLASIFICACON MAGERIT	FRECUENCIA DE LA AMENAZA	D	I	C	A	T
Host para solucion HA Vmware	[N.1] Fuego	5	100%				
	[N.*] Desastres naturales	5	100%				
	[N.2] Daños por agua	5	100%				
	[I.3] Contaminación mecánica	10	50%				
	[I.4] Contaminación electromagnética	10	20%				
	[I.5] Avería de origen físico o lógico	10	60%				
	[I.6] Corte del suministro eléctrico	5	100%				
	[I.7] Condiciones inadecuadas de Temperatura o humedad	5	20%				
	[I.11] Emanaciones electromagnéticas	10			5%		
	[E.2] Errores del administrador	5	100%	50%	50%		
Servidor de desarrollo en Amazon	[I.5] Avería de origen físico o lógico	5	100%				
Servidor telefonia interna	[N.1] Fuego	5	100%				
	[N.*] Desastres naturales	5	100%				
	[N.2] Daños por agua	5	100%				
	[I.3] Contaminación mecánica	10	50%				
	[I.4] Contaminación electromagnética	10	20%				
	[I.5] Avería de origen físico o lógico	10	60%				
	[I.6] Corte del suministro eléctrico	5	100%				
	[I.7] Condiciones inadecuadas de temperatura o humedad	50	20%				
	[E.2] Errores del administrador	5		20%	50%		
Servidor de Correo OWA	[I.5] Avería de origen físico o lógico	10	60%				
	[E.2] Errores del administrador	5		50%	50%		
Servidor servicios registrales	[I.5] Avería de origen físico o lógico	10	60%				
	[E.2] Errores del administrador	5	100%	75%	75%		
Servidor web servicios registrales	[I.5] Avería de origen físico o lógico	10	60%				
	[E.2] Errores del administrador	5	100%	75%	75%		
Servidor Web Registro Nacional de Turismo	[I.5] Avería de origen físico o lógico	10	60%				
	[E.2] Errores del administrador	5	75%	50%	50%		
Servidor Crear empresa	[I.5] Avería de origen físico o lógico	10	60%				
	[E.2] Errores del administrador	5	75%	50%	50%		
Servidor de bases de datos	[I.5] Avería de origen físico o lógico	10	60%				
	[E.2] Errores del administrador	5	100%	75%	75%		
Servidor de Correo zimbra	[I.5] Avería de origen físico o lógico	10	60%				
	[E.2] Errores del administrador	5	75%	50%	50%		
Enrutador Red RUES	[N.1] Fuego	5	100%				
	[N.*] Desastres naturales	5	100%				
	[N.2] Daños por agua	5	100%				
	[I.3] Contaminación mecánica	10	50%				
	[I.4] Contaminación electromagnética	10	20%				
	[I.5] Avería de origen físico o lógico	10	60%				
	[I.6] Corte del suministro eléctrico	5	100%				
	[I.7] Condiciones inadecuadas de temperatura o humedad	10	20%				
	[I.11] Emanaciones electromagnéticas	10			5%		
	[E.2] Errores del administrador	5	75%	50%	50%		

NOMBRE ACTIVO DE ACUERDO A LA EMPRESA	AMENAZA CLASIFICACON MAGERIT	FRECUENCIA DE LA AMENAZA	D	I	C	A	T
Enrutador ISP Principal Synapsis	[N.1] Fuego	5	100%				
	[N.*] Desastres naturales	5	100%				
	[N.2] Daños por agua	5	100%				
	[I.3] Contaminación mecánica	10	50%				
	[I.4] Contaminación electromagnética	10	20%				
	[I.5] Avería de origen físico o lógico	10	60%				
	[I.6] Corte del suministro eléctrico	5	100%				
	[I.7] Condiciones inadecuadas de temperatura o humedad	10	20%				
	[I.11] Emanaciones electromagnéticas	10			5%		
	[E.2] Errores del administrador	5	75%	50%	50%		
Acceso internet contingencia	[N.1] Fuego	5	100%				
	[N.*] Desastres naturales	5	100%				
	[N.2] Daños por agua	5	100%				
	[I.3] Contaminación mecánica	10	50%				
	[I.4] Contaminación electromagnética	10	20%				
	[I.5] Avería de origen físico o lógico	10	60%				
	[I.6] Corte del suministro eléctrico	5	100%				
	[I.7] Condiciones inadecuadas de temperatura o humedad	50	20%				
	[I.11] Emanaciones electromagnéticas	10			5%		
	[E.2] Errores del administrador	5	75%	50%	50%		
UTM Panorama	[N.1] Fuego	5	100%				
	[N.*] Desastres naturales	5	100%				
	[N.2] Daños por agua	5	100%				
	[I.3] Contaminación mecánica	10	50%				
	[I.4] Contaminación electromagnética	10	20%				
	[I.5] Avería de origen físico o lógico	10	60%				
	[I.6] Corte del suministro eléctrico	5	100%				
	[I.7] Condiciones inadecuadas de temperatura o humedad	50	20%				
	[I.11] Emanaciones electromagnéticas	10			5%		
	[E.2] Errores del administrador	5	75%	50%	50%		
UTM Datacenter	[N.1] Fuego	5	100%				
	[N.*] Desastres naturales	5	100%				
	[N.2] Daños por agua	5	100%				
	[I.3] Contaminación mecánica	10	50%				
	[I.4] Contaminación electromagnética	10	20%				
	[I.5] Avería de origen físico o lógico	10	60%				
	[I.6] Corte del suministro eléctrico	5	100%				
	[I.7] Condiciones inadecuadas de temperatura o humedad	5	20%				
	[I.11] Emanaciones electromagnéticas	10			5%		
	[E.2] Errores del administrador	5	100%	75%	75%		
Switch panorama LAN	[N.1] Fuego	5	100%				
	[N.*] Desastres naturales	5	100%				
	[N.2] Daños por agua	5	100%				
	[I.3] Contaminación mecánica	10	50%				
	[I.4] Contaminación electromagnética	10	20%				
	[I.5] Avería de origen físico o lógico	10	60%				
	[I.6] Corte del suministro eléctrico	5	100%				
	[I.7] Condiciones inadecuadas de temperatura o humedad	50	20%				
	[I.11] Emanaciones electromagnéticas	10			5%		
	[E.2] Errores del administrador	5	50%	50%	50%		
Switch panorama red RUES	[N.1] Fuego	5	100%				
	[N.*] Desastres naturales	5	100%				
	[N.2] Daños por agua	5	100%				
	[I.3] Contaminación mecánica	10	50%				
	[I.4] Contaminación electromagnética	10	20%				
	[I.5] Avería de origen físico o lógico	10	60%				
	[I.6] Corte del suministro eléctrico	5	100%				
	[I.7] Condiciones inadecuadas de temperatura o humedad	50	20%				
	[I.11] Emanaciones electromagnéticas	10			5%		
	[E.2] Errores del administrador	5	75%	50%	50%		

NOMBRE ACTIVO DE ACUERDO A LA EMPRESA	AMENAZA CLASIFICACON MAGERIT	FRECUENCIA DE LA AMENAZA	D	I	C	A	T
Switch Synapsis Lan	[N.1] Fuego	5	100%				
	[N.*] Desastres naturales	5	100%				
	[N.2] Daños por agua	5	100%				
	[I.3] Contaminación mecánica	10	50%				
	[I.4] Contaminación electromagnética	10	20%				
	[I.6] Corte del suministro eléctrico	5	100%				
	[I.7] Condiciones inadecuadas de temperatura o humedad	5	20%				
	[I.11] Emanaciones electromagnéticas	10			5%		
	[E.2] Errores del administrador	5	75%	50%	50%		
Robot de Cintas	[N.1] Fuego	5	100%				
	[N.*] Desastres naturales	5	100%				
	[N.2] Daños por agua	5	100%				
	[I.3] Contaminación mecánica	10	50%				
	[I.4] Contaminación electromagnética	10	20%				
	[I.6] Corte del suministro eléctrico	5	100%				
	[I.7] Condiciones inadecuadas de temperatura o humedad	5	20%				
	[I.11] Emanaciones electromagnéticas	10			5%		
	[E.2] Errores del administrador	5	20%	50%	50%		
sistemas de alimentación ininterrumpida	[N.1] Fuego	5	100%				
	[N.*] Desastres naturales	5	100%				
	[N.2] Daños por agua	5	100%				
	[I.3] Contaminación mecánica	10	50%				
	[I.4] Contaminación electromagnética	10	20%				
	[I.5] Avería de origen físico o lógico	10	60%				
	[I.6] Corte del suministro eléctrico	5	100%				
	[I.7] Condiciones inadecuadas de temperatura o humedad	5	20%				
	[I.9] Interrupción de otros servicios y suministros esenciales	5	5%				
	[I.11] Emanaciones electromagnéticas	10			5%		
Almacenamiento en red	[N.1] Fuego	5	100%				
	[N.*] Desastres naturales	5	100%				
	[N.2] Daños por agua	5	100%				
	[I.3] Contaminación mecánica	10	50%				
	[I.4] Contaminación electromagnética	10	20%				
	[I.6] Corte del suministro eléctrico	5	100%				
	[I.7] Condiciones inadecuadas de temperatura o humedad	5	20%				
	[I.10] Degradación de los soportes de almacenamiento de la información	5	75%				
	[I.11] Emanaciones electromagnéticas	10			5%		
	[E.2] Errores del administrador	5	100%	75%	50%		

G. Redes de comunicaciones — **DIMENSION / VALOR**

NOMBRE ACTIVO DE ACUERDO A LA EMPRESA	AMENAZA CLASIFICACON MAGERIT	FRECUENCIA DE LA AMENAZA	D	I	C	A	T
Wifi contingencia y navegacion libre	[I.8] Fallo de servicios de comunicaciones	50	20%				
	[A.6] Abuso de privilegios de acceso	3	50%	20%	20%		
Red corporativa de voz y datos	[I.8] Fallo de servicios de comunicaciones	50	50%				
	[A.6] Abuso de privilegios de acceso	3	75%	50%	50%		
Red Datacenter RUES	[I.8] Fallo de servicios de comunicaciones	50	50%				
	[A.6] Abuso de privilegios de acceso	3	40%	80%	50%		
Red LAN Datacenter	[I.8] Fallo de servicios de comunicaciones	50	100%				
	[A.6] Abuso de privilegios de acceso	3	100%	95%	95%		
Red de internet principal	[I.8] Fallo de servicios de comunicaciones	50	100%				
	[A.6] Abuso de privilegios de acceso	3	100%	90%	90%		
Red de navegacion privada interconexion nacional Camaras de Comercio	[I.8] Fallo de servicios de comunicaciones	50	50%				
	[A.6] Abuso de privilegios de acceso	3	80%	50%	50%		

H. Instalaciones			DIMENSION / VALOR				
NOMBRE ACTIVO DE ACUERDO A LA EMPRESA	AMENAZA CLASIFICACON MAGERIT	FRECUENCIA DE LA AMENAZA	D	I	C	A	T
Edificio panorama principal	[N.1] Fuego	5	100%				
	[N.*] Desastres naturales	5	50%				
	[N.2] Daños por agua	5	90%				
	[I.3] Contaminación mecánica	70	10%				
	[I.11] Emanaciones electromagnéticas	5			5%		
Edificio datacenter ZonaFranca Synapsis	[N.1] Fuego	5	100%				
	[N.*] Desastres naturales	5	100%				
	[N.2] Daños por agua	5	100%				
	[I.3] Contaminación mecánica	70	10%				
	[I.11] Emanaciones electromagnéticas	5			5%		

I. Personal			DIMENSION / VALOR				
NOMBRE ACTIVO DE ACUERDO A LA EMPRESA	AMENAZA CLASIFICACON MAGERIT	FRECUENCIA DE LA AMENAZA	D	I	C	A	T
Usuarios de atencion al cliente i E y administrativos de todas las jerarquias	[E.7] Deficiencias en la organización	50	75%				
	[A.28] Indisponibilidad del personal	5	50%	60%			
	[A.30] Ingeniería social (picaresca)	5	70%	85%			
Administrador de infraestructura	[E.7] Deficiencias en la organización	50	75%				
	[A.28] Indisponibilidad del personal	5	75%	70%			
	[A.30] Ingeniería social (picaresca)	5	70%	85%			
Equipo de desarrollo y soporte	[E.7] Deficiencias en la organización	50	75%				
	[A.28] Indisponibilidad del personal	5	95%	95%			
	[A.30] Ingeniería social (picaresca)	5	70%	85%			

7. AMENAZAS (IDENTIFICACIÓN Y VALORACIÓN)

Las amenazas para la Confederación Colombiana de Cámaras de Comercio deberán estar establecidas en márgenes de ocurrencia, lo cual se establecerá mediante la Tabla 4dondela frecuencia es determinada por valores incrementales en términos de tiempo:

Tabla 4: Escala de rango de frecuencia de amenazas

ESCALA DE RANGO DE FRECUENCIA DE AMENAZAS		
VULNERABILIDAD	RANGO	VALOR
Frecuencia muy alta	1 vez al día	100
Frecuencia alta	1 vez cada 1 semanas	70
Frecuencia media	1 vez cada 2 meses	50
Frecuencia baja	1 vez cada 6 meses	10
Frecuencia muy baja	1 vez al año	5

Una vez se ha establecido la escala de frecuencia es necesario definir la escala de impacto en los activos (Tabla 5). Los cuales estarán asociados a las dimensiones disponibilidad [D], integridad [I], confiabilidad [C], Autenticidad [A], y trazabilidad [T]:

Tabla 5: Escala de rango porcentual de impactos

ESCALA DE RANGO PORCENTUAL DE IMPACTOS		
IMPACTO	**VALOR CUANTITATIVO**	**IMPACTO ESTANDAR**
Muy Alto	100%	5
Alto	75%	4
Medio	50%	3
Bajo	20%	2
Muy Bajo	5%	1

Teniendo en cuenta las anteriores escalas y sus representaciones, se procederá a presentar la relación de amenazas por cada activo de la confederación, identificando su frecuencia e impacto.

La representación, como se consolida y tabula en la tabla número 6, se realizará de acuerdo al nombre con el cual el activo es reconocido bajo el estándar de la entidad:

Tabla 6: Amenazas, identificación y valoración

AMENAZAS IDENTIFICACION Y VALORACION							
A. Activos esenciales			**DIMENSION / PORCENTAJE**				
NOMBRE ACTIVO DE ACUERDO A LA EMPRESA	**AMENAZA CLASIFICACON MAGERIT**	**FRECUENCIA DE LA AMENAZA**	**D**	**I**	**C**	**A**	**T**
Información de las Cámaras de Comercio	[E.15] Alteración accidental de la información	5		75%			
	[E.18] Destrucción de información	2	75%				
Información de aplicaciones del servicio registral	[E.15] Alteración accidental de la información	5		75%			
	[E.18] Destrucción de información	2	70%				
Código fuente: diseño, planes de pruebas	[E.15] Alteración accidental de la información	5		50%			
	[E.18] Destrucción de información	2	50%				
Histórico codigo fuente de aplicaciones	[E.15] Alteración accidental de la información	5		50%			
	[E.18] Destrucción de información	2	50%				
Documentación de proyectos	[E.15] Alteración accidental de la información	5		50%			
	[E.18] Destrucción de información	2	60%				
Documentación de proyectos Convenios	[E.15] Alteración accidental de la información	5		50%			
	[E.18] Destrucción de información	2	70%				

		DIMENSION / VALOR				
AMENAZA CLASIFICACON MAGERIT	FRECUENCIA DE LA AMENAZA	D	I	C	A	T
[E.1] Errores de los usuarios	10	50%	75%	75%		
[E.1] Errores de los usuarios	5	50%	75%	75%		
[E.1] Errores de los usuarios	5	50%	75%	75%		
[E.1] Errores de los usuarios	5	75%	75%	75%		
[E.1] Errores de los usuarios	5	100%	100%	75%		

C. Claves Criptográficas

			DIMENSION / VALOR				
NOMBRE ACTIVO DE ACUERDO A LA EMPRESA	AMENAZA CLASIFICACON MAGERIT	FRECUENCIA DE LA AMENAZA	D	I	C	A	T
Claves de cifra pagos en linea	[E.2] Errores del administrador	5%	50%	75%	100%		
	[A.6] Abuso de privilegios de acceso	5%	75%	75%	75%		
Llaves criptograficas	[E.2] Errores del administrador	5%	50%	75%	100%		
	[A.6] Abuso de privilegios de acceso	5%	75%	75%	75%		

D. Servicios

			DIMENSION / VALOR				
NOMBRE ACTIVO DE ACUERDO A LA EMPRESA	AMENAZA CLASIFICACON MAGERIT	FRECUENCIA DE LA AMENAZA	D	I	C	A	T
Servicios prestados a las camaras de comercio bajo el modelo de acuerdo tecnologico	[E.2] Errores del administrador	5	75%	75%	100%		
	[A.6] Abuso de privilegios de acceso	5	75%	50%	80%		
Servicios prestados a los usuarios internos a traves del aplicativo web	[E.2] Errores del administrador	5	75%	75%	75%		
	[A.6] Abuso de privilegios de acceso	5	40%	50%	50%		
Servicio de internet ofrecido desde el datacenter	[E.2] Errores del administrador	5	100%	100%	50%		
	[A.6] Abuso de privilegios de acceso	5	50%	50%	90%		
Servidor de Correo zimbra	[E.2] Errores del administrador	5	50%	20%	50%		
	[A.6] Abuso de privilegios de acceso	5	30%	40%	50%		
Servidor de Correo OWA	[E.2] Errores del administrador	5	50%	75%	50%		
	[A.6] Abuso de privilegios de acceso	5	75%	50%	50%		
Bases de datos de los aplicativos web	[E.2] Errores del administrador	5	100%	100%	75%		
	[A.6] Abuso de privilegios de acceso	5	90%	80%	90%		
Nivel de acceso a traves de firewall desde conexiones personales	[E.2] Errores del administrador	5	100%	100%	75%		
	[A.6] Abuso de privilegios de acceso	5	100%	50%	50%		
Repositorios FTP del RUES	[E.2] Errores del administrador	5	20%	50%	50%		
	[A.6] Abuso de privilegios de acceso	5	30%	30%	45%		
Control de acceso a servicios de pagos electronico en SIPP	[E.2] Errores del administrador	5	50%	50%	75%		
	[A.6] Abuso de privilegios de acceso	5	60%	60%	50%		
Firmado automatico de certificados de camaras de comercio	[E.2] Errores del administrador	5	50%	50%	75%		
	[A.6] Abuso de privilegios de acceso	5	70%	95%	50%		
Conexión cifrada para la interconectividad protegida con la registraduria general de la nacion	[E.2] Errores del administrador	5	75%	100%	100%		
	[A.6] Abuso de privilegios de acceso	5	90%	100%	100%		

E. Aplicaciones			DIMENSION / VALOR				
CODIGO GRUPO DE ACTIVO MAGERIT	NOMBRE ACTIVO DE ACUERDO A LA EMPRESA	FRECUENCIA DE LA	D	I	C	A	T
Software desarrollado por la empresa.	[I.5] Avería de origen físico o lógico	10	60%				
	[E.2] Errores del administrador	10	75%	75%	75%		
	[E.20] Vulnerabilidades de los programas (software)	10	50%	50%	50%		
	[A.6] Abuso de privilegios de acceso	3	85%	85%	90%		
Software en pruebas desarrollado por la empresa	[I.5] Avería de origen físico o lógico	10	60%				
	[E.2] Errores del administrador	10	75%	50%	10%		
	[E.20] Vulnerabilidades de los programas (software)		75%	50%	50%		
	[A.6] Abuso de privilegios de acceso	3	85%	70%	90%		
Acuerdos de software con terceros	[I.5] Avería de origen físico o lógico	10	60%				
	[E.2] Errores del administrador	10	75%	75%	75%		
	[E.20] Vulnerabilidades de los programas (software)		75%	50%	50%		
	[A.6] Abuso de privilegios de acceso	3	85%	65%	90%		
Servidor servicios registrales	[I.5] Avería de origen físico o lógico	10	60%				
	[E.2] Errores del administrador	5	100%	75%	75%		
	[E.20] Vulnerabilidades de los programas (software)		75%	75%	75%		
	[A.6] Abuso de privilegios de acceso	3	88%	85%	90%		
Servidor web servicios registrales	[I.5] Avería de origen físico o lógico	10	60%				
	[E.2] Errores del administrador	5	100%	75%	100%		
	[E.20] Vulnerabilidades de los programas (software)		75%	50%	50%		
	[A.6] Abuso de privilegios de acceso	3	85%	85%	90%		
Servidor Web Registro Nacional de Turismo	[I.5] Avería de origen físico o lógico	10	60%				
	[E.2] Errores del administrador	5	100%	75%	50%		
	[E.20] Vulnerabilidades de los programas (software)		75%	75%	75%		
	[A.6] Abuso de privilegios de acceso	3	87%	85%	90%		
Servidor Crear empresa	[I.5] Avería de origen físico o lógico	10	60%				
	[E.2] Errores del administrador	5	100%	75%	75%		
	[E.20] Vulnerabilidades de los programas (software)		75%	75%	75%		
	[A.6] Abuso de privilegios de acceso	3	85%	85%	90%		
Outlook para conexión a servidor de correo interno	[I.5] Avería de origen físico o lógico	10	60%				
	[E.9] Errores de [re-]encaminamiento	10	50%				
	[E.2] Errores del administrador	5	5%	50%	75%		
	[E.9] Errores de [re-]encaminamiento	50		75%			
	[E.20] Vulnerabilidades de los programas (software)		20%	50%	50%		
	[A.6] Abuso de privilegios de acceso	3	89%	85%	90%		
Robot SMTP para aplicativos	[I.5] Avería de origen físico o lógico	10	60%				
	[E.9] Errores de [re-]encaminamiento	5	20%				
	[E.2] Errores del administrador	5	50%	50%	75%		
	[E.20] Vulnerabilidades de los programas (software)		30%	40%	40%		
	[A.6] Abuso de privilegios de acceso	3	85%	85%	90%		
Servicio de correo empresarial	[I.5] Avería de origen físico o lógico	10	60%				
	[E.8] Difusión de software dañino	1	20%				
	[E.2] Errores del administrador	5	75%	75%	100%		
	[E.9] Errores de [re-]encaminamiento	50		75%			
	[E.20] Vulnerabilidades de los programas (software)		50%	45%	45%		
	[A.6] Abuso de privilegios de acceso	3	52%	85%	90%		
Navicat Gold	[I.5] Avería de origen físico o lógico	10	60%				
	[E.8] Difusión de software dañino	1	5%				
	[E.2] Errores del administrador	5	5%	20%	50%		
	[E.20] Vulnerabilidades de los programas (software)		5%	10%	20%		
	[A.6] Abuso de privilegios de acceso	3	41%	85%	90%		
Sistema Operativo Servidores	[I.5] Avería de origen físico o lógico	10	60%				
	[E.2] Errores del administrador	5	100%	75%	75%		
	[E.20] Vulnerabilidades de los programas (software)		75%	50%	50%		
	[A.6] Abuso de privilegios de acceso	3	85%	85%	90%		

Sistema Operativo funcionarios	[I.5] Avería de origen físico o lógico	10	60%				
	[E.8] Difusión de software dañino	1	50%				
	[E.2] Errores del administrador	5	75%	50%	50%		
	[E.20] Vulnerabilidades de los programas (software)		75%	50%	50%		
	[A.6] Abuso de privilegios de acceso	3	52%	85%	90%		
Sistema Operativo Soportes	[I.5] Avería de origen físico o lógico	10	60%				
	[E.8] Difusión de software dañino	5	75%				
	[E.2] Errores del administrador	5	75%	75%	50%		
	[E.20] Vulnerabilidades de los programas (software)		75%	50%	50%		
	[A.6] Abuso de privilegios de acceso	3	85%	85%	90%		
Gestor plataforma de virtualización	[I.5] Avería de origen físico o lógico	10	60%				
	[E.2] Errores del administrador	5	100%	50%	50%		
	[E.20] Vulnerabilidades de los programas (software)		100%	75%	75%		
	[A.6] Abuso de privilegios de acceso	3	52%	85%	90%		

F. Equipos Informáticos

			DIMENSION / VALOR				
NOMBRE ACTIVO DE ACUERDO A LA EMPRESA	**AMENAZA CLASIFICACON MAGERIT**	**FRECUENCIA DE LA AMENAZA**	**D**	**I**	**C**	**A**	**T**
Host para solucion HA Vmware	[N.1] Fuego	5	100%				
	[N.*] Desastres naturales	5	100%				
	[N.2] Daños por agua	5	100%				
	[I.3] Contaminación mecánica	10	50%				
	[I.4] Contaminación electromagnética	10	20%				
	[I.5] Avería de origen físico o lógico	10	60%				
	[I.6] Corte del suministro eléctrico	5	100%				
	[I.7] Condiciones inadecuadas de Temperatura o humedad	5	20%				
	[I.11] Emanaciones electromagnéticas	10			5%		
	[E.2] Errores del administrador	5	100%	50%	50%		
Servidor de desarrollo en Amazon	[I.5] Avería de origen físico o lógico	5	100%				
Servidor telefonia interna	[N.1] Fuego	5	100%				
	[N.*] Desastres naturales	5	100%				
	[N.2] Daños por agua	5	100%				
	[I.3] Contaminación mecánica	10	50%				
	[I.4] Contaminación electromagnética	10	20%				
	[I.5] Avería de origen físico o lógico	10	60%				
	[I.6] Corte del suministro eléctrico	5	100%				
	[I.7] Condiciones inadecuadas de temperatura o humedad	50	20%				
	[E.2] Errores del administrador	5		20%	50%		
Servidor de Correo OWA	[I.5] Avería de origen físico o lógico	10	60%				
	[E.2] Errores del administrador	5		50%	50%		
Servidor servicios registrales	[I.5] Avería de origen físico o lógico	10	60%				
	[E.2] Errores del administrador	5	100%	75%	75%		
Servidor web servicios registrales	[I.5] Avería de origen físico o lógico	10	60%				
	[E.2] Errores del administrador	5	100%	75%	75%		
Servidor Web Registro Nacional de Turismo	[I.5] Avería de origen físico o lógico	10	60%				
	[E.2] Errores del administrador	5	75%	50%	50%		
Servidor Crear empresa	[I.5] Avería de origen físico o lógico	10	60%				
	[E.2] Errores del administrador	5	75%	50%	50%		
Servidor de bases de datos	[I.5] Avería de origen físico o lógico	10	60%				
	[E.2] Errores del administrador	5	100%	75%	75%		
Servidor de Correo zimbra	[I.5] Avería de origen físico o lógico	10	60%				
	[E.2] Errores del administrador	5	75%	50%	50%		
Enrutador Red RUES	[N.1] Fuego	5	100%				
	[N.*] Desastres naturales	5	100%				
	[N.2] Daños por agua	5	100%				
	[I.3] Contaminación mecánica	10	50%				
	[I.4] Contaminación electromagnética	10	20%				
	[I.5] Avería de origen físico o lógico	10	60%				
	[I.6] Corte del suministro eléctrico	5	100%				
	[I.7] Condiciones inadecuadas de temperatura o humedad	10	20%				
	[I.11] Emanaciones electromagnéticas	10			5%		
	[E.2] Errores del administrador	5	75%	50%	50%		

NOMBRE ACTIVO DE ACUERDO A LA EMPRESA	AMENAZA CLASIFICACON MAGERIT	FRECUENCIA DE LA AMENAZA	D	I	C	A	T
Enrutador ISP Principal Synapsis	[N.1] Fuego	5	100%				
	[N.*] Desastres naturales	5	100%				
	[N.2] Daños por agua	5	100%				
	[I.3] Contaminación mecánica	10	50%				
	[I.4] Contaminación electromagnética	10	20%				
	[I.5] Avería de origen físico o lógico	10	60%				
	[I.6] Corte del suministro eléctrico	5	100%				
	[I.7] Condiciones inadecuadas de temperatura o humedad	10	20%				
	[I.11] Emanaciones electromagnéticas	10			5%		
	[E.2] Errores del administrador	5	75%	50%	50%		
Acceso internet contingencia	[N.1] Fuego	5	100%				
	[N.*] Desastres naturales	5	100%				
	[N.2] Daños por agua	5	100%				
	[I.3] Contaminación mecánica	10	50%				
	[I.4] Contaminación electromagnética	10	20%				
	[I.5] Avería de origen físico o lógico	10	60%				
	[I.6] Corte del suministro eléctrico	5	100%				
	[I.7] Condiciones inadecuadas de temperatura o humedad	50	20%				
	[I.11] Emanaciones electromagnéticas	10			5%		
	[E.2] Errores del administrador	5	75%	50%	50%		
UTM Panorama	[N.1] Fuego	5	100%				
	[N.*] Desastres naturales	5	100%				
	[N.2] Daños por agua	5	100%				
	[I.3] Contaminación mecánica	10	50%				
	[I.4] Contaminación electromagnética	10	20%				
	[I.5] Avería de origen físico o lógico	10	60%				
	[I.6] Corte del suministro eléctrico	5	100%				
	[I.7] Condiciones inadecuadas de temperatura o humedad	50	20%				
	[I.11] Emanaciones electromagnéticas	10			5%		
	[E.2] Errores del administrador	5	75%	50%	50%		
UTM Datacenter	[N.1] Fuego	5	100%				
	[N.*] Desastres naturales	5	100%				
	[N.2] Daños por agua	5	100%				
	[I.3] Contaminación mecánica	10	50%				
	[I.4] Contaminación electromagnética	10	20%				
	[I.5] Avería de origen físico o lógico	10	60%				
	[I.6] Corte del suministro eléctrico	5	100%				
	[I.7] Condiciones inadecuadas de temperatura o humedad	5	20%				
	[I.11] Emanaciones electromagnéticas	10			5%		
	[E.2] Errores del administrador	5	100%	75%	75%		
Switch panorama LAN	[N.1] Fuego	5	100%				
	[N.*] Desastres naturales	5	100%				
	[N.2] Daños por agua	5	100%				
	[I.3] Contaminación mecánica	10	50%				
	[I.4] Contaminación electromagnética	10	20%				
	[I.5] Avería de origen físico o lógico	10	60%				
	[I.6] Corte del suministro eléctrico	5	100%				
	[I.7] Condiciones inadecuadas de temperatura o humedad	50	20%				
	[I.11] Emanaciones electromagnéticas	10			5%		
	[E.2] Errores del administrador	5	50%	50%	50%		
Switch panorama red RUES	[N.1] Fuego	5	100%				
	[N.*] Desastres naturales	5	100%				
	[N.2] Daños por agua	5	100%				
	[I.3] Contaminación mecánica	10	50%				
	[I.4] Contaminación electromagnética	10	20%				
	[I.5] Avería de origen físico o lógico	10	60%				
	[I.6] Corte del suministro eléctrico	5	100%				
	[I.7] Condiciones inadecuadas de temperatura o humedad	50	20%				
	[I.11] Emanaciones electromagnéticas	10			5%		
	[E.2] Errores del administrador	5	75%	50%	50%		

NOMBRE ACTIVO DE ACUERDO A LA EMPRESA	AMENAZA CLASIFICACON MAGERIT	FRECUENCIA DE LA AMENAZA	D	I	C	A	T
Switch Synapsis Lan	[N.1] Fuego	5	100%				
	[N.*] Desastres naturales	5	100%				
	[N.2] Daños por agua	5	100%				
	[I.3] Contaminación mecánica	10	50%				
	[I.4] Contaminación electromagnética	10	20%				
	[I.6] Corte del suministro eléctrico	5	100%				
	[I.7] Condiciones inadecuadas de temperatura o humedad	5	20%				
	[I.11] Emanaciones electromagnéticas	10			5%		
	[E.2] Errores del administrador	5	75%	50%	50%		
Robot de Cintas	[N.1] Fuego	5	100%				
	[N.*] Desastres naturales	5	100%				
	[N.2] Daños por agua	5	100%				
	[I.3] Contaminación mecánica	10	50%				
	[I.4] Contaminación electromagnética	10	20%				
	[I.6] Corte del suministro eléctrico	5	100%				
	[I.7] Condiciones inadecuadas de temperatura o humedad	5	20%				
	[I.11] Emanaciones electromagnéticas	10			5%		
	[E.2] Errores del administrador	5	20%	50%	50%		
sistemas de alimentación ininterrumpida	[N.1] Fuego	5	100%				
	[N.*] Desastres naturales	5	100%				
	[N.2] Daños por agua	5	100%				
	[I.3] Contaminación mecánica	10	50%				
	[I.4] Contaminación electromagnética	10	20%				
	[I.5] Avería de origen físico o lógico	10	60%				
	[I.6] Corte del suministro eléctrico	5	100%				
	[I.7] Condiciones inadecuadas de temperatura o humedad	5	20%				
	[I.9] Interrupción de otros servicios y suministros esenciales	5	5%				
	[I.11] Emanaciones electromagnéticas	10			5%		
Almacenamiento en red	[N.1] Fuego	5	100%				
	[N.*] Desastres naturales	5	100%				
	[N.2] Daños por agua	5	100%				
	[I.3] Contaminación mecánica	10	50%				
	[I.4] Contaminación electromagnética	10	20%				
	[I.6] Corte del suministro eléctrico	5	100%				
	[I.7] Condiciones inadecuadas de temperatura o humedad	5	20%				
	[I.10] Degradación de los soportes de almacenamiento de la información	5	75%				
	[I.11] Emanaciones electromagnéticas	10			5%		
	[E.2] Errores del administrador	5	100%	75%	50%		

G. Redes de comunicaciones

NOMBRE ACTIVO DE ACUERDO A LA EMPRESA	AMENAZA CLASIFICACON MAGERIT	FRECUENCIA DE LA AMENAZA	DIMENSION / VALOR D	I	C	A	T
Wifi contingencia y navegacion libre	[I.8] Fallo de servicios de comunicaciones	50	20%				
	[A.6] Abuso de privilegios de acceso	3	50%	20%	20%		
Red corporativa de voz y datos	[I.8] Fallo de servicios de comunicaciones	50	50%				
	[A.6] Abuso de privilegios de acceso	3	75%	50%	50%		
Red Datacenter RUES	[I.8] Fallo de servicios de comunicaciones	50	50%				
	[A.6] Abuso de privilegios de acceso	3	40%	80%	50%		
Red LAN Datacenter	[I.8] Fallo de servicios de comunicaciones	50	100%				
	[A.6] Abuso de privilegios de acceso	3	100%	95%	95%		
Red de internet principal	[I.8] Fallo de servicios de comunicaciones	50	100%				
	[A.6] Abuso de privilegios de acceso	3	100%	90%	90%		
Red de navegacion privada interconexion nacional Camaras de Comercio	[I.8] Fallo de servicios de comunicaciones	50	50%				
	[A.6] Abuso de privilegios de acceso	3	80%	50%	50%		

H. Instalaciones			DIMENSION / VALOR				
NOMBRE ACTIVO DE ACUERDO A LA EMPRESA	AMENAZA CLASIFICACON MAGERIT	FRECUENCIA DE LA AMENAZA	D	I	C	A	T
Edificio panorama principal	[N.1] Fuego	5	100%				
	[N.*] Desastres naturales	5	50%				
	[N.2] Daños por agua	5	90%				
	[I.3] Contaminación mecánica	70	10%				
	[I.11] Emanaciones electromagnéticas	5			5%		
Edificio datacenter ZonaFranca Synapsis	[N.1] Fuego	5	100%				
	[N.*] Desastres naturales	5	100%				
	[N.2] Daños por agua	5	100%				
	[I.3] Contaminación mecánica	70	10%				
	[I.11] Emanaciones electromagnéticas	5			5%		
I. Personal			DIMENSION / VALOR				
NOMBRE ACTIVO DE ACUERDO A LA EMPRESA	AMENAZA CLASIFICACON MAGERIT	FRECUENCIA DE LA AMENAZA	D	I	C	A	T
Usuarios de atencion al cliente i E y administrativos de todas las jerarquias	[E.7] Deficiencias en la organización	50	75%				
	[A.28] Indisponibilidad del personal	5	50%	60%			
	[A.30] Ingeniería social (picaresca)	5	70%	85%			
Administrador de infraestructura	[E.7] Deficiencias en la organización	50	75%				
	[A.28] Indisponibilidad del personal	5	75%	70%			
	[A.30] Ingeniería social (picaresca)	5	70%	85%			
Equipo de desarrollo y soporte	[E.7] Deficiencias en la organización	50	75%				
	[A.28] Indisponibilidad del personal	5	95%	95%			
	[A.30] Ingeniería social (picaresca)	5	70%	85%			

8. ANÁLISIS DE LAS SALVAGUARDAS

Para obtener el nivel de riesgo al cuál la entidad actualmente está sometida, es necesario tener en cuenta en el análisis de riesgos de acuerdo a las salvaguardas implantadas en la entidad. Estas salvaguardas afectan del siguiente modo al riesgo:

- Reduciendo la frecuencia de las amenazas: medidas preventivas para limitar la materialización de la amenaza.
- Limitando el impacto: medidas correctoras y en menor medida detectoras, las cuales mitigan el impacto ante la materialización de la amenaza o lo que es lo mismo, disminuyen el factor de degradación de valor.
-

Respecto a las salvaguardas aplicables de acuerdo al catálogo de MAGERIT en su punto 6 contempla un listado de salvaguardas en la siguiente escala propuesta (nulo, bajo, alto, completo).

Las salvaguardas elegidas para el análisis son las siguientes y se toman del Catalogo II de Magerit en su versión 3. Las mismas fueron elegidas partiendo de la clasificación y de su efectiva aplicación en el objetivo de mitigar en la medida de lo posible la materialización de una amenaza.

Se realizó un análisis detallado, de cada activo, identificando los servicios definidos en el alcance y dándoles un peso personalizado, de esa forma es mucho más aproximado el análisis y la aplicación correspondiente de la salvaguarda.

En la tabla 7, se presenta el establecimiento exhaustivo de las salvaguardas dependiendo de cada grupo de activos:

Tabla 7: Establecimiento de salvaguardas

ESTABLECIMIENTO DE LAS SALVAGUARDAS					
A. Activos esenciales					
CODIGO GRUPO DE ACTIVO MAGERIT	**NOMBRE GRUPO DE ACTIVO MAGERIT**	**CODIGO ACTIVO DE ACUERDO A LA EMPRESA**	**NOMBRE ACTIVO DE ACUERDO A LA EMPRESA**	**TIPO PROTECCION**	**DESCRIPCION SALVAGUARDAS**
[vr]	Datos vitales	[I_Clientes_Camaras]	Información de las Cámaras de Comercio	H.AC	Control de acceso lógico
		[I_Aplicativo_SII]	Información de aplicaciones del servicio registral	H.AC	Control de acceso lógico
[classified]	Datos clasificados	[C_F_Aplicaciones]	Código fuente: diseño, planes de pruebas	H.tools.SFV	Verificación de las funciones de seguridad
		[H_CodigoFuente]	Histórico codigo fuente de aplicaciones	H.tools.SFV	Verificación de las funciones de seguridad
		[D_Proyectos]	Documentación de proyectos	H.AC	Control de acceso lógico
		[D_Proyectos_convenios]	Documentación de proyectos Convenios	H.AC	Control de acceso lógico
B. Datos/Información					
CODIGO GRUPO DE ACTIVO MAGERIT	**NOMBRE GRUPO DE ACTIVO MAGERIT**	**CODIGO ACTIVO DE ACUERDO A LA EMPRESA**	**NOMBRE ACTIVO DE ACUERDO A LA EMPRESA**	**TIPO PROTECCION**	**DESCRIPCION SALVAGUARDAS**
[files]	Ficheros	[F_clientes internos]	Archivos de clientes internos	H.tools.AV	Herramienta contra código dañino
				D.A	Copias de seguridad de los datos (backup)
[conf]	Datos de configuracion	[D_Doc_infraestructura]	Datos de configuracion de servidores y equipos	H.tools.AV	Herramienta contra código dañino
				D.A	Copias de seguridad de los datos (backup)
[int]	Datos de gestión interna	[D_GestionProyectos]	Datos de Gestión de proyectos	H.tools.AV	Herramienta contra código dañino
				D.A	Copias de seguridad de los datos (backup)
[password]	Credenciales	[Pass_usuarios]	Credenciales de acceso tanto para usuarios dentro de la	H.tools.AV	Herramienta contra código dañino
				D.A	Copias de seguridad de los datos (backup)
				D.C	Cifrado de la información
[acl]	Datos de control de acceso	[Control_acceso_datacenter_Synapsis]	Controles de acceso al CPD.	H.AC	Control de acceso lógico
				D.A	Copias de seguridad de los datos (backup)
		[Control_acceso_datacenter_col_XV]	Controles de acceso al CPD.	H.IA	Control de acceso lógico
				D.A	Copias de seguridad de los datos (backup)
C. Claves Criptográficas	Conectividad para certificados virtuales de las Cámaras de Comercio				
CODIGO GRUPO DE ACTIVO MAGERIT	**NOMBRE GRUPO DE ACTIVO MAGERIT**	**CODIGO ACTIVO DE ACUERDO A LA EMPRESA**	**NOMBRE ACTIVO DE ACUERDO A LA EMPRESA**	**TIPO PROTECCION**	**DESCRIPCION SALVAGUARDAS**
[encrypt]	Claves de cifra	[CC_plataformas_pagos_electro]	Claves de cifra pagos en linea	K.DS	Gestión de claves de firma de información
[sign]	Llaves de firma	[llaves_p12]	Llaves criptograficas	K.DS	Gestión de claves de firma de información

D. Servicios	Servicios tecnologicos ofrecidos por parte de la Confederacion Colombiana				
CODIGO GRUPO DE ACTIVO MAGERIT	**NOMBRE GRUPO DE ACTIVO MAGERIT**	**CODIGO ACTIVO DE ACUERDO A LA EMPRESA**	**NOMBRE ACTIVO DE ACUERDO A LA EMPRESA**	**TIPO PROTECCION**	**DESCRIPCION SALVAGUARDAS**
[ext]	A usuarios externos (bajo una relación contractual)	[S_U_Externo]	Servicios prestados a las camaras de	S.A	Aseguramiento de la disponibilidad
				S.start	Aceptación y puesta en operación
[int]	Interno (a usuarios de la propia organización)	[S_U_Interno]	Servicios prestados a los usuarios internos a	S.A	Aseguramiento de la disponibilidad
				S.start	Aceptación y puesta en operación
[www]	World wide web	[S_Internet]	Servicio de internet ofrecido desde el	S.A	Aseguramiento de la disponibilidad
				S.start	Aceptación y puesta en operación
[email]	Correo electrónico	[S_correo]	Servidor de Correo zimbra	S.A	Aseguramiento de la disponibilidad
				S.start	Aceptación y puesta en operación
		[S_correo_ext]	Servidor de Correo OWA	S.A	Aseguramiento de la disponibilidad
				S.start	Aceptación y puesta en operación
				S.email	Protección del correo electrónico
[file]	Almacenamiento de ficheros	S_A_Bases de datos]	Bases de datos de los aplicativos web	S.A	Aseguramiento de la disponibilidad
				S.start	Aceptación y puesta en operación
[ipm]	Gestión de privilegios	[G_privilegios]	Nivel de acceso a traves de firewall desde	S.A	Aseguramiento de la disponibilidad
				S.start	Aceptación y puesta en operación
[edi]	Intercambio electrónico de datos	[D_D_Electronicamente]	Repositorios FTP del RUES	S.A	Aseguramiento de la disponibilidad
				S.start	Aceptación y puesta en operación
[idm]	Gestión de identidades	[G_Identidades]	Control de acceso a servicios de pagos	S.A	Aseguramiento de la disponibilidad
				S.start	Aceptación y puesta en operación
[pki]	PKI - infraestructura de clave pública	[Firmado_p12]	Firmado automatico de certificados de camaras	S.A	Aseguramiento de la disponibilidad
				S.start	Aceptación y puesta en operación
	PKI - infraestructura de clave pública	[Conexión_Cifrada_Regist]	Conexión cifrada para la interconectividad	S.A	Aseguramiento de la disponibilidad
				S.start	Aceptación y puesta en operación

E. Aplicaciones	Los acuerdos tecnologicos celebrados por confecamaras con las caámaras de comercio de				
CODIGO GRUPO DE ACTIVO MAGERIT	**NOMBRE GRUPO DE ACTIVO MAGERIT**	**CODIGO ACTIVO DE ACUERDO A LA EMPRESA**	**NOMBRE ACTIVO DE ACUERDO A LA EMPRESA**	**TIPO PROTECCION**	**DESCRIPCION SALVAGUARDAS**
[prp]	Desarrollo propio (in house)	[Soft_propio]	Software desarrollado por la empresa.	SW.A	Copias de seguridad (backup)
		[Soft_pruebas]	Software en pruebas desarrollado por la empresa	SW.A	Copias de seguridad (backup)
[Sub]	desarrollo a medida (subcontratado)	[Soft_tercerizado]	Acuerdos de software con terceros	SW.A	Copias de seguridad (backup)
				SW.CM	Cambios (actualizaciones y mantenimiento)
[app]	Servidor de	[Server_App_Sirep]	Servidor servicios registrales	SW.A	Copias de seguridad (backup)
				SW.start	Puesta en producción
				SW.SC	Se aplican perfiles de seguridad
	aplicaciones	[Server_App_SII]	Servidor web servicios registrales	SW.A	Copias de seguridad (backup)
				SW.start	Puesta en producción
				SW.SC	Se aplican perfiles de seguridad
		[Server_App_RNT]	Servidor Web Registro Nacional de Turismo	SW.A	Copias de seguridad (backup)
				SW.start	Puesta en producción
				SW.SC	Se aplican perfiles de seguridad
		[Server_App_CAE]	Servidor Crear empresa	SW.A	Copias de seguridad (backup)
				SW.start	Puesta en producción
				SW.SC	Se aplican perfiles de seguridad
[email_client]	Cliente de correo electrónico	[Cliente_correo]	Outlook para conexión a servidor de correo interno	SW.A	Copias de seguridad (backup)
[email_server]	Servidor de correo electrónico	[Server_correo_zimbra]	Robot SMTP para aplicativos	SW.A	Copias de seguridad (backup)
		[Server_correo_owa]	Servicio de correo empresarial	SW.A	Copias de seguridad (backup)
[dbms]	Sistema de gestión de bases de datos	[DBMS_MySQL]	Navicat Gold	SW.A	Copias de seguridad (backup)
		[DBMS_PostgresSQL]		SW.A	Copias de seguridad (backup)
		[DBMS_SQLServer]		SW.A	Copias de seguridad (backup)
		[DBMS_Adabast]		SW.A	Copias de seguridad (backup)
[os]	Sistema operativo	[SO_Linux]	Sistema Operativo Servidores	SW.A	Copias de seguridad (backup)
		[SO_Windows]	Sistema Operativo funcionarios	SW.A	Copias de seguridad (backup)
		[SO_OSX]	Sistema Operativo Soportes	SW.A	Copias de seguridad (backup)
[hypervisor]	Gestor de máquinas virtuales	[VM_Ware]	Gestor plataforma de virtualización	PS.A	Aseguramiento de la disponibilidad

F. Equipos Informáticos Entran en consideración los equipos informaticos que permiten realizar la operación en Confecámaras.

CODIGO GRUPO DE ACTIVO MAGERIT	NOMBRE GRUPO DE ACTIVO MAGERIT	CODIGO ACTIVO DE ACUERDO A LA EMPRESA	NOMBRE ACTIVO DE ACUERDO A LA EMPRESA	TIPO PROTECCION	DESCRIPCION SALVAGUARDAS
[hosts]	Grandes equipos (Servidor web, Servidor de bases de datos, servidores de aplicación)	[Host_IBM_1]	Host para solucion HA Vmware	HW	Protección de los Equipos Informáticos
				HW.op	Operación
[mid]	Equipos medios (Equipos de desarrollo conectados a través de red inalámbrica por red 802.1x)	[Server_desa_Amazon]	Servidor de desarrollo en Amazon	HW	Protección de los Equipos Informáticos
		[Server_asterisk]	Servidor telefonia interna	HW	Protección de los Equipos Informáticos
		[Server_correo_owa]	Servidor de Correo OWA	HW	Protección de los Equipos Informáticos
[vhost]	Grandes equipos (Servidor web, Servidor de bases de datos, servidores de aplicación)	[Server_App_Sirep]	Servidor servicios registrales	HW.SC	Se aplican perfiles de seguridad
		[Server_App_SII]	Servidor web servicios registrales	HW.SC	Se aplican perfiles de seguridad
		[Server_App_RNT]	Servidor Web Registro Nacional de Turismo	HW.SC	Se aplican perfiles de seguridad
		[Server_App_CAE]	Servidor Crear empresa	HW.SC	Se aplican perfiles de seguridad
		[Server_MySQL]	Servidor de bases de datos	HW.SC	Se aplican perfiles de seguridad
		[Server_correo_zimbra]	Servidor de Correo zimbra	HW.SC	Se aplican perfiles de seguridad
[router]	Enrutadores	[Router_Level3_Panorama]	Enrutador Red RUES	HW	Protección de los Equipos Informáticos
		[Router_Synapsis]	Enrutador ISP Principal Synapsis	HW	Protección de los Equipos Informáticos
[wap]	Punto de acceso inalámbrico	[Router_Une_Internet]	Acceso internet contingencia	HW	Protección de los Equipos Informáticos
[Firewall]	Cortafuegos	[Juniper_Panrorama]	UTM Panorama	HW	Protección de los Equipos Informáticos
		[Juniper_synapsis]	UTM Datacenter	HW	Protección de los Equipos Informáticos
[switch]	conmutadores	[Sw_panorama_lan]	Switch panorama LAN	HW	Protección de los Equipos Informáticos
	conmutadores	[Sw_panorama_Rues]	Switch panorama red RUES	HW	Protección de los Equipos Informáticos
	conmutadores	[Sw_Synapsis_lan]	Switch Synapsis Lan	HW	Protección de los Equipos Informáticos
[tape]	cinta magnética	[Tape_LTO5	Cintas Magneticas LTO5	HW	Protección de los Equipos Informáticos
[ups]	sistemas de alimentación ininterrumpida	[Ups_Panorama]	Ups Sede Panorama	HW	Protección de los Equipos Informáticos
				AUX.A	Aseguramiento de la disponibilidad
[robot][tape]	Robot de Cintas	[Ts_2900]	Robot Cintas Datacenter	HW	Protección de los Equipos Informáticos
[san]	almacenamiento en red	[DS_3400]	Almacenamiento 1	HW	Protección de los Equipos Informáticos
		[V3700]	Almacenamiento 2	HW	Protección de los Equipos Informáticos

G. Redes de comunicaciones

CODIGO GRUPO DE ACTIVO MAGERIT	NOMBRE GRUPO DE ACTIVO MAGERIT	CODIGO ACTIVO DE ACUERDO A LA EMPRESA	NOMBRE ACTIVO DE ACUERDO A LA EMPRESA	TIPO PROTECCION	DESCRIPCION SALVAGUARDAS
[wifi]	Red inalámbrica	[Wifi_www]	Wifi contingencia y navegacion libre	Seguridad Wireless (WiFi)	Seguridad Wireless (WiFi)
[LAN]	Red local	[LAN_corporativa_panorama]	Red corporativa de voz y datos	COM.A	Aseguramiento de la disponibilidad
		[LAN_coporativa_Datacenter_RUES]	Red Datacenter RUES	COM.A	Aseguramiento de la disponibilidad
		[LAN_coporativa_datacenter]	Red LAN Datacenter	COM.A	Aseguramiento de la disponibilidad
[Internet]	Internet	[Wan_coporativa]	Red de internet principal	COM.A	Aseguramiento de la disponibilidad
				COM.SC	Se aplican perfiles de seguridad
				COM.op	Operación
				COM.DS	Segregación de las redes en dominios
				IP.SPP	Sistema de protección perimetral
		[Wan_RUES]	Red de navegacion privada interconexion nacional Camaras de Comercio	COM.A	Aseguramiento de la disponibilidad

H. Instalaciones

CODIGO GRUPO DE ACTIVO MAGERIT	NOMBRE GRUPO DE ACTIVO MAGERIT	CODIGO ACTIVO DE ACUERDO A LA EMPRESA	NOMBRE ACTIVO DE ACUERDO A LA EMPRESA	TIPO PROTECCION	DESCRIPCION SALVAGUARDAS
[building]	Edificio	[Edif_Panorama]	Edificio panorama principal	L.design	Diseño
				L.AC	Control de los accesos físicos
		[Edif_Datacenter]	Edificio datacenter ZonaFranca Synapsis	L.design	Diseño
				L.depth	Defensa en profundidad
				L.AC	Control de los accesos físicos
				L.A	Aseguramiento de la disponibilidad
				BC.DRP	Plan de Recuperación de Desastres (DRP)

I. Personal

CODIGO GRUPO DE ACTIVO MAGERIT	NOMBRE GRUPO DE ACTIVO MAGERIT	CODIGO ACTIVO DE ACUERDO A LA EMPRESA	NOMBRE ACTIVO DE ACUERDO A LA EMPRESA	TIPO PROTECCION	DESCRIPCION SALVAGUARDAS
[ui]	Usuarios internos	[U_nivel1]	Usuarios de atencion al cliente i E y	PS.AT	Formación y concienciación
				PS.A	Aseguramiento de la disponibilidad
[adm]	Administradores de sistemas	[U_Nivel_3]	Administrador de infraestructura	PS.AT	Formación y concienciación
				PS.A	Aseguramiento de la disponibilidad
[des]	Desarrolladores programadores	[U_Nivel_2]	Equipo de desarrollo y soporte	PS.AT	Formación y concienciación
				PS.A	Aseguramiento de la disponibilidad

9. INFORME DE EVALUACIÓN DE RIESGOS

El cálculo de riesgo establece lo que existe entre el riesgo y la probabilidad a partir de la frecuencia y el impacto que tendría en la organización la materialización del riesgo.

La tabla número 8, evidencia la relación de los riesgos para cada dimensión de seguridad a partir de la frecuencia y la probabilidad de ocurrencia de las amenazas determinadas para los activos:

Tabla 8: Cálculo del riesgo

CALCULO DEL RIESGO

RIESGO		PROBABILIDAD				
		MB	B	M	A	MA
IMPACTO	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

El cálculo del riesgo y la premura con la que hay que actuar se establece en la denominación que el nivel da a cada activo y cuya estimación del riesgo se

representa de manera taxativa en la tabla número 9, donde se presentan los valores para, el impacto, la probabilidad , y el riesgo:

Tabla 9: Estimación del riesgo

ESTIMACIÓN DEL RIESGO					
IMPACTO		**PROBABILIDAD**		**RIESGO**	
MA	muy alto	**MA**	practicamente seguro	**MA**	crítico
A	alto	**A**	probable	**A**	importante
M	medio	**M**	posible	**M**	apreciable
B	bajo	**B**	poco probable	**B**	bajo
MB	muy bajo	**MB**	muy raro	**MB**	despreciable

A continuación se ilustra la tabla general (Tabla número 10) del análisis de riesgos con la estimación del riesgo correspondiente:

Tabla 10: informe valoración del riesgo

INFORME DE VALORACIÓN DE RIESGOS				
A. Activos esenciales		**RIESGO CUALITATIVO / DIMENSIÓN**		
AMENAZA CLASIFICACON MAGERIT	**NOMBRE ACTIVO DE ACUERDO A LA EMPRESA**	**D**	**I**	**C**
[E.15] Alteración accidental de la información	Información de las Cámaras de Comercio		MB	
[E.18] Destrucción de información	Información de las Cámaras de Comercio	MB		
[E.15] Alteración accidental de la información	Información de aplicaciones del servicio registral		MB	
[E.18] Destrucción de información	Información de aplicaciones del servicio registral	MB		
[E.15] Alteración accidental de la información	Código fuente: diseño, planes de pruebas		MB	
[E.18] Destrucción de información	Código fuente: diseño, planes de pruebas	MB		
[E.15] Alteración accidental de la información	Histórico codigo fuente de aplicaciones		MB	
[E.18] Destrucción de información	Histórico codigo fuente de aplicaciones	MB		
[E.15] Alteración accidental de la información	Documentación de proyectos		MB	
[E.18] Destrucción de información	Documentación de proyectos	MB		
[E.15] Alteración accidental de la información	Documentación de proyectos Convenios		MB	
[E.18] Destrucción de información	Documentación de proyectos Convenios	MB		
B. Datos/Información		**RIESGO CUALITATIVO / DIMENSIÓN**		
AMENAZA CLASIFICACON MAGERIT	**NOMBRE ACTIVO DE ACUERDO A LA EMPRESA**	**D**	**I**	**C**
[E.1] Errores de los usuarios	Archivos de clientes internos	MB	MB	MB
[E.1] Errores de los usuarios	Datos de configuracion de servidores y equipos	MB	MB	MB
[E.1] Errores de los usuarios	Datos de Gestión de proyectos	MB	MB	MB
[E.1] Errores de los usuarios	Credenciales de acceso tanto para usuarios dentro de la empresa como de forma remota	MB	MB	MB
[E.1] Errores de los usuarios	Controles de acceso al CPD SYN	MB	MB	MB
[E.1] Errores de los usuarios	Controles de acceso al C15	MB	MB	MB

C. Claves Criptográficas		RIESGO CUALITATIVO / DIMENSIÓN		
AMENAZA CLASIFICACON MAGERIT	NOMBRE ACTIVO DE ACUERDO A LA EMPRESA	D	I	C
[E.2] Errores del administrador	Claves de cifra pagos en linea	MB	MB	MB
[A.6] Abuso de privilegios de acceso	Claves de cifra pagos en linea	MB	MB	MB
[E.2] Errores del administrador	Llaves criptograficas	MB	MB	MB
[A.6] Abuso de privilegios de acceso	Llaves criptograficas	MB	MB	MB
D. Servicios		**RIESGO CUALITATIVO / DIMENSIÓN**		
AMENAZA CLASIFICACON MAGERIT	NOMBRE ACTIVO DE ACUERDO A LA EMPRESA	D	I	C
[E.2] Errores del administrador	Servicios prestados a las camaras de comercio bajo el modelo de acuerdo tecnologico	MB	MB	MB
[A.6] Abuso de privilegios de acceso	Servicios prestados a las camaras de comercio bajo el modelo de acuerdo tecnologico	MB	MB	MB
[E.2] Errores del administrador	Servicios prestados a los usuarios internos a traves del aplicativo web	MB	MB	MB
[A.6] Abuso de privilegios de acceso	Servicios prestados a los usuarios internos a traves del aplicativo web	MB	MB	MB
[E.2] Errores del administrador	Servicio de internet ofrecido desde el datacenter	MB	MB	MB
[A.6] Abuso de privilegios de acceso	Servicio de internet ofrecido desde el datacenter	MB	MB	MB
[E.2] Errores del administrador	Servidor de Correo zimbra	MB	MB	MB
[A.6] Abuso de privilegios de acceso	Servidor de Correo zimbra	MB	MB	MB
[E.2] Errores del administrador	Servidor de Correo OWA	MB	MB	MB
[A.6] Abuso de privilegios de acceso	Servidor de Correo OWA	MB	MB	MB
[E.2] Errores del administrador	Bases de datos de los aplicativos web	MB	MB	MB
[A.6] Abuso de privilegios de acceso	Bases de datos de los aplicativos web	MB	MB	MB
[E.2] Errores del administrador	Nivel de acceso a traves de firewall desde conexiones personales	MB	MB	MB
[A.6] Abuso de privilegios de acceso	Nivel de acceso a traves de firewall desde conexiones personales	MB	MB	MB
[E.2] Errores del administrador	Repositorios FTP del RUES	MB	MB	MB
[A.6] Abuso de privilegios de acceso	Repositorios FTP del RUES	MB	MB	MB
[E.2] Errores del administrador	Control de acceso a servicios de pagos electronico en SIPP	MB	MB	MB
[A.6] Abuso de privilegios de acceso	Control de acceso a servicios de pagos electronico en SIPP	MB	MB	MB
[E.2] Errores del administrador	Firmado automatico de certificados de camaras de comercio	MB	MB	MB
[A.6] Abuso de privilegios de acceso	Firmado automatico de certificados de camaras de comercio	MB	MB	MB
[E.2] Errores del administrador	Conexión cifrada para la interconectividad protegida con la registraduria general de la nacion	MB	MB	MB
[A.6] Abuso de privilegios de acceso	Conexión cifrada para la interconectividad protegida con la registraduria general de la nacion	MB	MB	MB

E. Aplicaciones		RIESGO CUALITATIVO / DIMENSIÓN		
NOMBRE ACTIVO DE ACUERDO A LA EMPRESA	CODIGO GRUPO DE ACTIVO MAGERIT	D	I	C
[I.5] Avería de origen físico o lógico	Software desarrollado por la empresa.	B		
[E.2] Errores del administrador	Software desarrollado por la empresa.	B	B	B
[E.20] Vulnerabilidades de los programas (software)	Software desarrollado por la empresa.	B	B	B
[A.6] Abuso de privilegios de acceso	Software desarrollado por la empresa.	MB	MB	MB
[I.5] Avería de origen físico o lógico	Software en pruebas desarrollado por la empresa	B		
[E.2] Errores del administrador	Software en pruebas desarrollado por la empresa	B	B	MB
[E.20] Vulnerabilidades de los programas (software)	Software en pruebas desarrollado por la empresa	MB	MB	MB
[A.6] Abuso de privilegios de acceso	Software en pruebas desarrollado por la empresa	MB	MB	MB
[I.5] Avería de origen físico o lógico	Acuerdos de software con terceros	B		
[E.2] Errores del administrador	Acuerdos de software con terceros	B	B	B
[E.20] Vulnerabilidades de los programas (software)	Acuerdos de software con terceros	MB	MB	MB
[A.6] Abuso de privilegios de acceso	Acuerdos de software con terceros	MB	MB	MB
[I.5] Avería de origen físico o lógico	Servidor servicios registrales	B		
[E.2] Errores del administrador	Servidor servicios registrales	MB	MB	MB
[E.20] Vulnerabilidades de los programas (software)	Servidor servicios registrales	MB	MB	MB
[A.6] Abuso de privilegios de acceso	Servidor servicios registrales	MB	MB	MB
[I.5] Avería de origen físico o lógico	Servidor web servicios registrales	B		
[E.2] Errores del administrador	Servidor web servicios registrales	MB	MB	MB
[E.20] Vulnerabilidades de los programas (software)	Servidor web servicios registrales	MB	MB	MB
[A.6] Abuso de privilegios de acceso	Servidor web servicios registrales	MB	MB	MB
[I.5] Avería de origen físico o lógico	Servidor Web Registro Nacional de Turismo	B		
[E.2] Errores del administrador	Servidor Web Registro Nacional de Turismo	MB	MB	MB
[E.20] Vulnerabilidades de los programas (software)	Servidor Web Registro Nacional de Turismo	MB	MB	MB
[A.6] Abuso de privilegios de acceso	Servidor Web Registro Nacional de Turismo	MB	MB	MB
[I.5] Avería de origen físico o lógico	Servidor Crear empresa	B		
[E.2] Errores del administrador	Servidor Crear empresa	MB	MB	MB
[E.20] Vulnerabilidades de los programas (software)	Servidor Crear empresa	MB	MB	MB
[A.6] Abuso de privilegios de acceso	Servidor Crear empresa	MB	MB	MB
[I.5] Avería de origen físico o lógico	Outlook para conexión a servidor de correo interno	B		
[E.9] Errores de [re-]encaminamiento	Outlook para conexión a servidor de correo interno	B		

AMENAZA CLASIFICACON MAGERIT	NOMBRE ACTIVO DE ACUERDO A LA EMPRESA	D	I	C
[E.2] Errores del administrador	Outlook para conexión a servidor de correo interno	MB	MB	MB
[E.9] Errores de [re-]encaminamiento	Outlook para conexión a servidor de correo interno		M	
[E.20] Vulnerabilidades de los programas (software)	Outlook para conexión a servidor de correo interno	MB	MB	MB
[A.6] Abuso de privilegios de acceso	Outlook para conexión a servidor de correo interno	MB	MB	MB
[I.5] Avería de origen físico o lógico	Robot SMTP para aplicativos	B		
[E.9] Errores de [re-]encaminamiento	Robot SMTP para aplicativos	MB		
[E.2] Errores del administrador	Robot SMTP para aplicativos	MB	MB	MB
[E.20] Vulnerabilidades de los programas (software)	Robot SMTP para aplicativos	MB	MB	MB
[A.6] Abuso de privilegios de acceso	Robot SMTP para aplicativos	MB	MB	MB
[I.5] Avería de origen físico o lógico	Servicio de correo empresarial	B		
[E.8] Difusión de software dañino	Servicio de correo empresarial	MB		
[E.2] Errores del administrador	Servicio de correo empresarial	MB	MB	MB
[E.9] Errores de [re-]encaminamiento	Servicio de correo empresarial		M	
[E.20] Vulnerabilidades de los programas (software)	Servicio de correo empresarial	MB	MB	MB
[A.6] Abuso de privilegios de acceso	Servicio de correo empresarial	MB	MB	MB
[I.5] Avería de origen físico o lógico	Navicat Gold	B		
[E.8] Difusión de software dañino	Navicat Gold	MB		
[E.2] Errores del administrador	Navicat Gold	MB	MB	MB
[E.20] Vulnerabilidades de los programas (software)	Navicat Gold	MB	MB	MB
[A.6] Abuso de privilegios de acceso	Navicat Gold	MB	MB	MB
[I.5] Avería de origen físico o lógico	Sistema Operativo Servidores	B		
[E.2] Errores del administrador	Sistema Operativo Servidores	MB	MB	MB
[E.20] Vulnerabilidades de los programas (software)	Sistema Operativo Servidores	MB	MB	MB
[A.6] Abuso de privilegios de acceso	Sistema Operativo Servidores	MB	MB	MB
[I.5] Avería de origen físico o lógico	Sistema Operativo funcionarios	B		
[E.8] Difusión de software dañino	Sistema Operativo funcionarios	MB		
[E.2] Errores del administrador	Sistema Operativo funcionarios	MB	MB	MB
[E.20] Vulnerabilidades de los programas (software)	Sistema Operativo funcionarios	MB	MB	MB
[A.6] Abuso de privilegios de acceso	Sistema Operativo funcionarios	MB	MB	MB
[I.5] Avería de origen físico o lógico	Sistema Operativo Soportes	B		
[E.8] Difusión de software dañino	Sistema Operativo Soportes	MB		
[E.2] Errores del administrador	Sistema Operativo Soportes	MB	MB	MB
[E.20] Vulnerabilidades de los programas (software)	Sistema Operativo Soportes	MB	MB	MB
[A.6] Abuso de privilegios de acceso	Sistema Operativo Soportes	MB	MB	MB
[I.5] Avería de origen físico o lógico	Gestor plataforma de virtualización	B		
[E.2] Errores del administrador	Gestor plataforma de virtualización	MB	MB	MB
[E.20] Vulnerabilidades de los programas (software)	Gestor plataforma de virtualización	MB	MB	MB
[A.6] Abuso de privilegios de acceso	Gestor plataforma de virtualización	MB	MB	MB

F. Equipos Informáticos		RIESGO CUALITATIVO / DIMENSIÓN		
AMENAZA CLASIFICACON MAGERIT	NOMBRE ACTIVO DE ACUERDO A LA EMPRESA	D	I	C
[N.1] Fuego	Host para solucion HA Vmware	MB		
[N.*] Desastres naturales	Host para solucion HA Vmware	MB		
[N.2] Daños por agua	Host para solucion HA Vmware	MB		
[I.3] Contaminación mecánica	Host para solucion HA Vmware	B		
[I.4] Contaminación electromagnética	Host para solucion HA Vmware	MB		
[I.5] Avería de origen físico o lógico	Host para solucion HA Vmware	B		
[I.6] Corte del suministro eléctrico	Host para solucion HA Vmware	MB		
[I.7] Condiciones inadecuadas de Temperatura o humedad	Host para solucion HA Vmware	MB		
[I.11] Emanaciones electromagnéticas	Host para solucion HA Vmware			MB
[E.2] Errores del administrador	Host para solucion HA Vmware	MB	MB	MB
[I.5] Avería de origen físico o lógico	Servidor de desarrollo en Amazon	MB		
[N.1] Fuego	Servidor telefonia interna	MB		
[N.*] Desastres naturales	Servidor telefonia interna	MB		
[N.2] Daños por agua	Servidor telefonia interna	MB		
[I.3] Contaminación mecánica	Servidor telefonia interna	B		
[I.4] Contaminación electromagnética	Servidor telefonia interna	MB		
[I.5] Avería de origen físico o lógico	Servidor telefonia interna	B		
[I.6] Corte del suministro eléctrico	Servidor telefonia interna	MB		
[I.7] Condiciones inadecuadas de temperatura o humedad	Servidor telefonia interna	B		
[E.2] Errores del administrador	Servidor telefonia interna		MB	MB
[I.5] Avería de origen físico o lógico	Servidor de Correo OWA	B		
[E.2] Errores del administrador	Servidor de Correo OWA		MB	MB
[I.5] Avería de origen físico o lógico	Servidor servicios registrales	B		
[E.2] Errores del administrador	Servidor servicios registrales	MB	MB	MB
[I.5] Avería de origen físico o lógico	Servidor web servicios registrales	B		
[E.2] Errores del administrador	Servidor web servicios registrales	MB	MB	MB
[I.5] Avería de origen físico o lógico	Servidor Web Registro Nacional de Turismo	B		
[E.2] Errores del administrador	Servidor Web Registro Nacional de Turismo	MB	MB	MB
[I.5] Avería de origen físico o lógico	Servidor Crear empresa	B		
[E.2] Errores del administrador	Servidor Crear empresa	MB	MB	MB
[I.5] Avería de origen físico o lógico	Servidor de bases de datos	B		
[E.2] Errores del administrador	Servidor de bases de datos	MB	MB	MB
[I.5] Avería de origen físico o lógico	Servidor de Correo zimbra	B		
[E.2] Errores del administrador	Servidor de Correo zimbra	MB	MB	MB
[N.1] Fuego	Enrutador Red RUES	MB		
[N.*] Desastres naturales	Enrutador Red RUES	MB		
[N.2] Daños por agua	Enrutador Red RUES	MB		
[I.3] Contaminación mecánica	Enrutador Red RUES	B		
[I.4] Contaminación electromagnética	Enrutador Red RUES	MB		
[I.5] Avería de origen físico o lógico	Enrutador Red RUES	B		
[I.6] Corte del suministro eléctrico	Enrutador Red RUES	MB		
[I.7] Condiciones inadecuadas de temperatura o humedad	Enrutador Red RUES	MB		
[I.11] Emanaciones electromagnéticas	Enrutador Red RUES			MB
[E.2] Errores del administrador	Enrutador Red RUES	MB	MB	MB
[N.1] Fuego	Enrutador ISP Principal Synapsis	MB		
[N.*] Desastres naturales	Enrutador ISP Principal Synapsis	MB		
[N.2] Daños por agua	Enrutador ISP Principal Synapsis	MB		
[I.3] Contaminación mecánica	Enrutador ISP Principal Synapsis	B		

AMENAZA CLASIFICACON MAGERIT	NOMBRE ACTIVO DE ACUERDO A LA EMPRESA	D	I	C
[I.4] Contaminación electromagnética	Enrutador ISP Principal Synapsis	MB		
[I.5] Avería de origen físico o lógico	Enrutador ISP Principal Synapsis	B		
[I.6] Corte del suministro eléctrico	Enrutador ISP Principal Synapsis	MB		
[I.7] Condiciones inadecuadas de temperatura o humedad	Enrutador ISP Principal Synapsis	MB		
[I.11] Emanaciones electromagnéticas	Enrutador ISP Principal Synapsis			MB
[E.2] Errores del administrador	Enrutador ISP Principal Synapsis	MB	MB	MB
[N.1] Fuego	Acceso internet contingencia	MB		
[N.*] Desastres naturales	Acceso internet contingencia	MB		
[N.2] Daños por agua	Acceso internet contingencia	MB		
[I.3] Contaminación mecánica	Acceso internet contingencia	B		
[I.4] Contaminación electromagnética	Acceso internet contingencia	MB		
[I.5] Avería de origen físico o lógico	Acceso internet contingencia	B		
[I.6] Corte del suministro eléctrico	Acceso internet contingencia	MB		
[I.7] Condiciones inadecuadas de temperatura o humedad	Acceso internet contingencia	M		
[I.11] Emanaciones electromagnéticas	Acceso internet contingencia			MB
[E.2] Errores del administrador	Acceso internet contingencia	MB	MB	MB
[N.1] Fuego	UTM Panorama	MB		
[N.*] Desastres naturales	UTM Panorama	MB		
[N.2] Daños por agua	UTM Panorama	MB		
[I.3] Contaminación mecánica	UTM Panorama	B		
[I.4] Contaminación electromagnética	UTM Panorama	MB		
[I.5] Avería de origen físico o lógico	UTM Panorama	B		
[I.6] Corte del suministro eléctrico	UTM Panorama	MB		
[I.7] Condiciones inadecuadas de temperatura o humedad	UTM Panorama	M		
[I.11] Emanaciones electromagnéticas	UTM Panorama			MB
[E.2] Errores del administrador	UTM Panorama	MB	MB	MB
[N.1] Fuego	UTM Datacenter	MB		
[N.*] Desastres naturales	UTM Datacenter	MB		
[N.2] Daños por agua	UTM Datacenter	MB		
[I.3] Contaminación mecánica	UTM Datacenter	B		
[I.4] Contaminación electromagnética	UTM Datacenter	MB		
[I.5] Avería de origen físico o lógico	UTM Datacenter	B		
[I.6] Corte del suministro eléctrico	UTM Datacenter	MB		
[I.7] Condiciones inadecuadas de temperatura o humedad	UTM Datacenter	MB		
[I.11] Emanaciones electromagnéticas	UTM Datacenter			MB
[E.2] Errores del administrador	UTM Datacenter	MB	MB	MB
[N.1] Fuego	Switch panorama LAN	MB		
[N.*] Desastres naturales	Switch panorama LAN	MB		
[N.2] Daños por agua	Switch panorama LAN	MB		
[I.3] Contaminación mecánica	Switch panorama LAN	B		

AMENAZA CLASIFICACON MAGERIT	NOMBRE ACTIVO DE ACUERDO A LA EMPRESA	D	I	C
[I.4] Contaminación electromagnética	Switch panorama LAN	MB		
[I.5] Avería de origen físico o lógico	Switch panorama LAN	B		
[I.6] Corte del suministro eléctrico	Switch panorama LAN	MB		
[I.7] Condiciones inadecuadas de temperatura o humedad	Switch panorama LAN	B		
[I.11] Emanaciones electromagnéticas	Switch panorama LAN			MB
[E.2] Errores del administrador	Switch panorama LAN	MB	MB	MB
[N.1] Fuego	Switch panorama red RUES	MB		
[N.*] Desastres naturales	Switch panorama red RUES	MB		
[N.2] Daños por agua	Switch panorama red RUES	MB		
[I.3] Contaminación mecánica	Switch panorama red RUES	B		
[I.4] Contaminación electromagnética	Switch panorama red RUES	MB		
[I.5] Avería de origen físico o lógico	Switch panorama red RUES	B		
[I.6] Corte del suministro eléctrico	Switch panorama red RUES	MB		
[I.7] Condiciones inadecuadas de temperatura o humedad	Switch panorama red RUES	B		
[I.11] Emanaciones electromagnéticas	Switch panorama red RUES			MB
[E.2] Errores del administrador	Switch panorama red RUES	MB	MB	MB
[N.1] Fuego	Switch Synapsis Lan	MB		
[N.*] Desastres naturales	Switch Synapsis Lan	MB		
[N.2] Daños por agua	Switch Synapsis Lan	MB		
[I.3] Contaminación mecánica	Switch Synapsis Lan	B		
[I.4] Contaminación electromagnética	Switch Synapsis Lan	MB		
[I.6] Corte del suministro eléctrico	Switch Synapsis Lan	MB		
[I.7] Condiciones inadecuadas de temperatura o humedad	Switch Synapsis Lan	MB		
[I.11] Emanaciones electromagnéticas	Switch Synapsis Lan			MB
[E.2] Errores del administrador	Switch Synapsis Lan	MB	MB	MB
[N.1] Fuego	Robot de Cintas	MB		
[N.*] Desastres naturales	Robot de Cintas	MB		
[N.2] Daños por agua	Robot de Cintas	MB		
[I.3] Contaminación mecánica	Robot de Cintas	B		
[I.4] Contaminación electromagnética	Robot de Cintas	MB		
[I.7] Condiciones inadecuadas de temperatura o humedad	Robot de Cintas	MB		
[I.11] Emanaciones electromagnéticas	Robot de Cintas			MB
[E.2] Errores del administrador	Robot de Cintas	MB	MB	MB
[N.1] Fuego	sistemas de alimentación ininterrumpida	MB		
[N.*] Desastres naturales	sistemas de alimentación ininterrumpida	MB		
[N.2] Daños por agua	sistemas de alimentación ininterrumpida	MB		
[I.3] Contaminación mecánica	sistemas de alimentación ininterrumpida	B		
[I.4] Contaminación electromagnética	sistemas de alimentación ininterrumpida	MB		
[I.5] Avería de origen físico o lógico	sistemas de alimentación ininterrumpida	B		
[I.6] Corte del suministro eléctrico	sistemas de alimentación ininterrumpida	MB		

AMENAZA CLASIFICACON MAGERIT	NOMBRE ACTIVO DE ACUERDO A LA EMPRESA	D	I	C
[I.7] Condiciones inadecuadas de temperatura o humedad	sistemas de alimentación ininterrumpida	MB		
[I.9] Interrupción de otros servicios y suministros esenciales	sistemas de alimentación ininterrumpida	MB		
[I.11] Emanaciones electromagnéticas	sistemas de alimentación ininterrumpida			MB
[N.1] Fuego	Almacenamiento en red	MB		
[N.*] Desastres naturales	Almacenamiento en red	MB		
[N.2] Daños por agua	Almacenamiento en red	MB		
[I.3] Contaminación mecánica	Almacenamiento en red	B		
[I.4] Contaminación electromagnética	Almacenamiento en red	MB		
[I.6] Corte del suministro eléctrico	Almacenamiento en red	MB		
[I.7] Condiciones inadecuadas de temperatura o humedad	Almacenamiento en red	MB		
[I.10] Degradación de los soportes de almacenamiento de la información	Almacenamiento en red	MB		
[I.11] Emanaciones electromagnéticas	Almacenamiento en red			MB
[E.2] Errores del administrador	Almacenamiento en red	MB	MB	MB

G. Redes de comunicaciones — RIESGO CUALITATIVO / DIMENSIÓN

AMENAZA CLASIFICACON MAGERIT	NOMBRE ACTIVO DE ACUERDO A LA EMPRESA	D	I	C
[I.8] Fallo de servicios de comunicaciones	Wifi contingencia y navegacion libre	B		
[A.6] Abuso de privilegios de acceso	Wifi contingencia y navegacion libre	MB	MB	MB
[I.8] Fallo de servicios de comunicaciones	Red corporativa de voz y datos	A		
[A.6] Abuso de privilegios de acceso	Red corporativa de voz y datos	MB	MB	MB
[I.8] Fallo de servicios de comunicaciones	Red Datacenter RUES	A		
[A.6] Abuso de privilegios de acceso	Red Datacenter RUES	MB	MB	MB
[I.8] Fallo de servicios de comunicaciones	Red LAN Datacenter	MA		
[A.6] Abuso de privilegios de acceso	Red LAN Datacenter	MB	MB	MB
[I.8] Fallo de servicios de comunicaciones	Red de internet principal	MA		
[A.6] Abuso de privilegios de acceso	Red de internet principal	MB	MB	MB
[I.8] Fallo de servicios de comunicaciones	Red de navegacion privada interconexion nacional Camaras de Comercio	A		
[A.6] Abuso de privilegios de acceso	Red de navegacion privada interconexion nacional Camaras de Comercio	MB	MB	MB

H. Instalaciones — RIESGO CUALITATIVO / DIMENSIÓN

AMENAZA CLASIFICACON MAGERIT	NOMBRE ACTIVO DE ACUERDO A LA EMPRESA	D	I	C
[N.1] Fuego	Edificio panorama principal	MB		
[N.*] Desastres naturales	Edificio panorama principal	MB		
[N.2] Daños por agua	Edificio panorama principal	MB		
[I.3] Contaminación mecánica	Edificio panorama principal	B		
[I.11] Emanaciones electromagnéticas	Edificio panorama principal			MB
[N.1] Fuego	Edificio datacenter ZonaFranca Synapsis	MB		
[N.*] Desastres naturales	Edificio datacenter ZonaFranca Synapsis	MB		
[N.2] Daños por agua	Edificio datacenter ZonaFranca Synapsis	MB		
[I.3] Contaminación mecánica	Edificio datacenter ZonaFranca Synapsis	B		
[I.11] Emanaciones electromagnéticas	Edificio datacenter ZonaFranca Synapsis			MB

I. Personal		RIESGO CUALITATIVO / DIMENSIÓN		
AMENAZA CLASIFICACON MAGERIT	NOMBRE ACTIVO DE ACUERDO A LA EMPRESA	D	I	C
[E.7] Deficiencias en la organización	Usuarios de atencion al cliente i E y administrativos de todas las jerarquias	M		
[A.28] Indisponibilidad del personal	Usuarios de atencion al cliente i E y administrativos de todas las jerarquias	MB	MB	
[A.30] Ingeniería social (picaresca)	Usuarios de atencion al cliente i E y administrativos de todas las jerarquias	MB	MB	
[E.7] Deficiencias en la organización	Administrador de infraestructura	A		
[A.28] Indisponibilidad del personal	Administrador de infraestructura	MB	MB	
[A.30] Ingeniería social (picaresca)	Administrador de infraestructura	MB	MB	
[E.7] Deficiencias en la organización	Equipo de desarrollo y soporte	A		
[A.28] Indisponibilidad del personal	Equipo de desarrollo y soporte	MB	MB	
[A.30] Ingeniería social (picaresca)	Equipo de desarrollo y soporte	MB	MB	

10. RESULTADOS DEL ANÁLISIS DE RIESGOS

De acuerdo al análisis arrojado en la valoración del riesgos obtenido desde la metodología Magerit Versión 3, se puede observar que aunque son pocos los focos que atención inmediata, son puntos que entregarían un impacto bastante notable en el caso de que se llegaran a presentar, teniendo en cuenta que es el sistema de comunicaciones principal el que sufriría de manera más comprometedora:

- Red Lan Datacenter
- Red de Internet Principal (Datacenter)

Ambos nodos son el “back bone” con el Datacenter Synapsis, donde se ofrecen los servicios a los clientes principales, y que de sufrir una afectación continua respecto al tiempo de duración, habría que recurrir de manera indispensable al plan de recuperación de desastres incluido dentro de este Sistema de Gestión de Seguridad Informática.

Como segundo aspecto notable del análisis de riesgos, se entregan alarmas de nivel “Medio” y “Alto” en el grupo de “Personal” y que por su naturaleza deben ser atendidos cuanto antes ya que una deficiencia en la organización deja una notable falencia de sincronización entre las partes.

Por otro lado se detecta una falencia de usuarios en el nivel de “Deficiencias de la organización”, puntualmente en los activos:

- Administrador de Infraestructura y
- Equipo de desarrollo

Los cuales por la relevancia de sus roles operativos y misión en la organización, dejan de entrever una vulnerabilidad que necesariamente necesita atención.

5.6.1 MATRIZ DE RIESGOS

Una vez presentado todo el análisis de riesgos propio del SGSI se entrega la matriz de riesgos en la cual según la tabla número 11, considerando la medición del riesgo inherente y el riesgo residual, como dos partes fundamentales de evidencia de la gestión. Por un lado se entrega el riesgo inherente, como característica propia del activo y del cual no se tienen en cuenta los controles.

Por otro lado está el riesgo residual el cual es el riesgo que permanece, incluso cuando se han implementado controles. Es de manera apropiada indicar que el nivel de riesgo al que está sometido una compañía no puede mitigarse totalmente.

Esto conlleva a buscar un balance del nivel de recursos y mecanismos que es necesario optimizar para minimizar o mitigar dichos riesgos y un cierto nivel de confianza que se puede considerar suficiente (nivel de riesgo aceptable).

El riesgo residual se aprecia como aquello que separa a la confederación de la seguridad absoluta, tal como se muestra en la tabla número11:

Tabla número 11: Matriz de riesgos del SGSI

MATRIZ DE RIESGOS DEL SGSI - RIESGO INHERENTE											
N	Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Medición - Riesgo Inherente						
					Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
1	Información de las Cámaras de Comercio	Información de las Cámaras de Comercio	Información de las Cámaras de Comercio sobre el activo Información de las Cámaras de Comercio	[E.15] Alteración accidental de la información	Improbable	Menor	1	0,5	0,5	11	Baja
2	Información de las Cámaras de Comercio	Información de las Cámaras de Comercio	Información de las Cámaras de Comercio sobre el activo [E.18] Destrucción de información	[E.18] Destrucción de información	Poco Probable	Menor	1,3	0,5	0,65	14	Baja
3	Información de aplicaciones del servicio registral	Información de aplicaciones del servicio registral	Información de aplicaciones del servicio registral sobre el activo [E.15] Alteración accidental de la	[E.15] Alteración accidental de la información	Improbable	Menor	1	0,5	0,5	11	Baja

N	Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Medición - Riesgo Inherente						
					Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
			información								
4	Información de aplicaciones del servicio registral	Información de aplicaciones del servicio registral	Información de aplicaciones del servicio registral sobre el activo [E.18] Destrucción de información	[E.18] Destrucción de información	Improbable	Moderado	1	0,68	0,68	15	Baja
5	Código fuente: diseño, planes de pruebas	Código fuente: diseño, planes de pruebas	Código fuente: diseño, planes de pruebas sobre el activo [E.15] Alteración accidental de la información	[E.15] Alteración accidental de la información	Probable	Menor	1,35	0,5	0,675	15	Baja
6	Código fuente: diseño, planes de pruebas	Código fuente: diseño, planes de pruebas	Código fuente: diseño, planes de pruebas sobre el activo [E.18] Destrucción de información	[E.18] Destrucción de información	Improbable	Menor	1	0,5	0,5	11	Baja
7	Histórico código fuente de aplicaciones	Histórico código fuente de aplicaciones	Histórico código fuente de aplicaciones sobre el activo [E.15] Alteración accidental de la información	[E.15] Alteración accidental de la información	Improbable	Menor	1	0,5	0,5	11	Baja
8	Histórico código fuente de aplicaciones	Histórico código fuente de aplicaciones	Histórico código fuente de aplicaciones sobre el activo [E.18] Destrucción de información	[E.18] Destrucción de información	Improbable	Menor	1	0,5	0,5	11	Baja
9	Documentación de proyectos	Documentación de proyectos	Documentación de proyectos sobre el activo [E.15] Alteración accidental de la información	[E.15] Alteración accidental de la información	Improbable	Menor	1	0,5	0,5	11	Baja
10	Documentación de proyectos	Documentación de proyectos	Documentación de proyectos sobre el activo [E.18] Destrucción de información	[E.18] Destrucción de información	Improbable	Menor	1	0,5	0,5	11	Baja
11	Documentación de proyectos Convenios	Documentación de proyectos Convenios	Documentación de proyectos Convenios sobre el activo [E.15] Alteración accidental de la información	[E.15] Alteración accidental de la información	Improbable	Menor	1	0,5	0,5	11	Baja

N	Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Medición - Riesgo Inherente						
					Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
12	Documentación de proyectos Convenios	Documentación de proyectos Convenios	Documentación de proyectos Convenios sobre el activo [E.18] Destrucción de información	[E.18] Destrucción de información	Poco Probable	Moderado	1,3	0,68	0,884	31	Media
13	Archivos de clientes internos	Archivos de clientes internos	Archivos de clientes internos sobre el activo [E.1] Errores de los usuarios	[E.1] Errores de los usuarios	Improbable	Moderado	1	0,68	0,68	15	Baja
14	Datos de configuración de servidores y equipos	Datos de configuración de servidores y equipos	Datos de configuración de servidores y equipos sobre el activo [E.1] Errores de los usuarios	[E.1] Errores de los usuarios	Poco Probable	Menor	1,3	0,5	0,65	14	Baja
15	Datos de Gestión de proyectos	Datos de Gestión de proyectos	Datos de Gestión de proyectos sobre el activo [E.1] Errores de los usuarios	[E.1] Errores de los usuarios	Improbable	Menor	1	0,5	0,5	11	Baja
16	Credenciales de acceso tanto para usuarios dentro de la empresa como de forma remota	Credenciales de acceso tanto para usuarios dentro de la empresa como de forma remota	Credenciales de acceso tanto para usuarios dentro de la empresa como de forma remota sobre el activo [E.1] Errores de los usuarios	[E.1] Errores de los usuarios	Improbable	Menor	1	0,5	0,5	11	Baja
17	Controles de acceso al CPD SYN	Controles de acceso al CPD SYN	Controles de acceso al CPD SYN sobre el activo [E.1] Errores de los usuarios	[E.1] Errores de los usuarios	Improbable	Menor	1	0,5	0,5	11	Baja
18	Controles de acceso al C15	Controles de acceso al C15	Controles de acceso al C15 sobre el activo [E.1] Errores de los usuarios	[E.1] Errores de los usuarios	Improbable	Menor	1	0,5	0,5	11	Baja
19	Claves de cifra pagos en línea	Claves de cifra pagos en línea	Claves de cifra pagos en línea sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja
20	Claves de cifra pagos en línea	Claves de cifra pagos en línea	Claves de cifra pagos en línea sobre el activo [A.6] Abuso de privilegios de acceso	[A.6] Abuso de privilegios de acceso	Improbable	Menor	1	0,5	0,5	11	Baja
21	Llaves criptográficas	Llaves criptográficas	Llaves criptográficas sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Poco Probable	Menor	1,3	0,5	0,65	14	Baja

N	Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Medición - Riesgo Inherente						
					Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
22	Llaves criptográficas	Llaves criptograficas	Llaves criptograficas sobre el activo [A.6] Abuso de privilegios de acceso	[A.6] Abuso de privilegios de acceso	Improbable	Moderado	1	0,68	0,68	15	Baja
23	Servicios prestados a las camaras de comercio bajo el modelo de acuerdo tecnologico	Servicios prestados a las camaras de comercio bajo el modelo de acuerdo tecnologico	Servicios prestados a las camaras de comercio bajo el modelo de acuerdo tecnologico sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja
24	Servicios prestados a las camaras de comercio bajo el modelo de acuerdo tecnologico	Servicios prestados a las camaras de comercio bajo el modelo de acuerdo tecnologico	Servicios prestados a las camaras de comercio bajo el modelo de acuerdo tecnologico sobre el activo [A.6] Abuso de privilegios de acceso	[A.6] Abuso de privilegios de acceso	Improbable	Menor	1	0,5	0,5	11	Baja
25	Servicios prestados a los usuarios internos a traves del aplicativo web	Servicios prestados a los usuarios internos a traves del aplicativo web	Servicios prestados a los usuarios internos a traves del aplicativo web sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja
26	Servicios prestados a los usuarios internos a traves del aplicativo web	Servicios prestados a los usuarios internos a traves del aplicativo web	Servicios prestados a los usuarios internos a traves del aplicativo web sobre el activo [A.6] Abuso de privilegios de acceso	[A.6] Abuso de privilegios de acceso	Poco Probable	Menor	1,3	0,5	0,65	14	Baja
27	Servicio de internet ofrecido desde el datacenter	Servicio de internet ofrecido desde el datacenter	Servicio de internet ofrecido desde el datacenter sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja
28	Servicio de internet ofrecido desde el datacenter	Servicio de internet ofrecido desde el datacenter	Servicio de internet ofrecido desde el datacenter sobre el activo [A.6] Abuso de privilegios de acceso	[A.6] Abuso de privilegios de acceso	Improbable	Moderado	1	0,68	0,68	15	Baja

N	Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Medición - Riesgo Inherente						
					Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
29	Servidor de Correo zimbra	Servidor de Correo zimbra	Servidor de Correo zimbra sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja
30	Servidor de Correo zimbra	Servidor de Correo zimbra	Servidor de Correo zimbra sobre el activo [A.6] Abuso de privilegios de acceso	[A.6] Abuso de privilegios de acceso	Poco Probable	Menor	1,3	0,5	0,65	14	Baja
31	Servidor de Correo OWA	Servidor de Correo OWA	Servidor de Correo OWA sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja
32	Servidor de Correo OWA	Servidor de Correo OWA	Servidor de Correo OWA sobre el activo [A.6] Abuso de privilegios de acceso	[A.6] Abuso de privilegios de acceso	Improbable	Menor	1	0,5	0,5	11	Baja
33	Bases de datos de los aplicativos web	Bases de datos de los aplicativos web	Bases de datos de los aplicativos web sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja
34	Bases de datos de los aplicativos web	Bases de datos de los aplicativos web	Bases de datos de los aplicativos web sobre el activo [A.6] Abuso de privilegios de acceso	[A.6] Abuso de privilegios de acceso	Improbable	Moderado	1	0,68	0,68	15	Baja
35	Nivel de acceso a traves de firewall desde conexiones personales	Nivel de acceso a traves de firewall desde conexiones personales	Nivel de acceso a traves de firewall desde conexiones personales sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja
36	Nivel de acceso a traves de firewall desde conexiones personales	Nivel de acceso a traves de firewall desde conexiones personales	Nivel de acceso a traves de firewall desde conexiones personales sobre el activo [A.6] Abuso de privilegios de acceso	[A.6] Abuso de privilegios de acceso	Poco Probable	Menor	1,3	0,5	0,65	14	Baja
37	Repositorios FTP del RUES	Repositorios FTP del RUES	Repositorios FTP del RUES sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja
38	Repositorios FTP del RUES	Repositorios FTP del RUES	Repositorios FTP del RUES sobre el activo [A.6] Abuso de privilegios de	[A.6] Abuso de privilegios de acceso	Improbable	Menor	1	0,5	0,5	11	Baja

N	Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Medición - Riesgo Inherente						
					Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
			acceso								
39	Control de acceso a servicios de pagos electronico en SIPP	Control de acceso a servicios de pagos electronico en SIPP	Control de acceso a servicios de pagos electronico en SIPP sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja
40	Control de acceso a servicios de pagos electronico en SIPP	Control de acceso a servicios de pagos electronico en SIPP	Control de acceso a servicios de pagos electronico en SIPP sobre el activo [A.6] Abuso de privilegios de acceso	[A.6] Abuso de privilegios de acceso	Improbable	Menor	1	0,5	0,5	11	Baja
41	Firmado automatico de certificados de camaras de comercio	Firmado automatico de certificados de camaras de comercio	Firmado automatico de certificados de camaras de comercio sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja
42	Firmado automatico de certificados de camaras de comercio	Firmado automatico de certificados de camaras de comercio	Firmado automatico de certificados de camaras de comercio sobre el activo [A.6] Abuso de privilegios de acceso	[A.6] Abuso de privilegios de acceso	Improbable	Moderado	1	0,68	0,68	15	Baja
43	Conexión cifrada para la interconectividad protegida con la registraduría general de la nacion	Conexión cifrada para la interconectividad protegida con la registraduría general de la nación	Conexión cifrada para la interconectividad protegida con la registraduría general de la nación sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja
44	Conexión cifrada para la interconectividad protegida con la registraduria general de la nacion	Conexión cifrada para la interconectividad protegida con la registraduria general de la nacion	Conexión cifrada para la interconectividad protegida con la registraduria general de la nacion sobre el activo [A.6] Abuso de privilegios de acceso	[A.6] Abuso de privilegios de acceso	Improbable	Menor	1	0,5	0,5	11	Baja
45	Software desarrollado por la	Software desarrollado por la	Software desarrollado por la empresa.	[I.5] Avería de origen físico o lógico	Improbable	Menor	1	0,5	0,5	11	Baja

N	Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Medición - Riesgo Inherente						
					Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
	empresa.	empresa.	sobre el activo [I.5] Avería de origen físico o lógico								
46	Software desarrollado por la empresa.	Software desarrollado por la empresa.	Software desarrollado por la empresa. sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Poco Probable	Menor	1,3	0,5	0,65	14	Baja
47	Software desarrollado por la empresa.	Software desarrollado por la empresa.	Software desarrollado por la empresa. sobre el activo [E.20] Vulnerabilidades de los programas (software)	[E.20] Vulnerabilidades de los programas (software)	Improbable	Menor	1	0,5	0,5	11	Baja
48	Software desarrollado por la empresa.	Software desarrollado por la empresa.	Software desarrollado por la empresa. sobre el activo [A.6] Abuso de privilegios de acceso	[A.6] Abuso de privilegios de acceso	Improbable	Menor	1	0,5	0,5	11	Baja
49	Software en pruebas desarrollado por la empresa	Software en pruebas desarrollado por la empresa	Software en pruebas desarrollado por la empresa sobre el activo [I.5] Avería de origen físico o lógico	[I.5] Avería de origen físico o lógico	Improbable	Menor	1	0,5	0,5	11	Baja
50	Software en pruebas desarrollado por la empresa	Software en pruebas desarrollado por la empresa	Software en pruebas desarrollado por la empresa sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja
51	Software en pruebas desarrollado por la empresa	Software en pruebas desarrollado por la empresa	Software en pruebas desarrollado por la empresa sobre el activo [E.20] Vulnerabilidades de los programas (software)	[E.20] Vulnerabilidades de los programas (software)	Improbable	Menor	1	0,5	0,5	11	Baja
52	Software en pruebas desarrollado por la empresa	Software en pruebas desarrollado por la empresa	Software en pruebas desarrollado por la empresa sobre el activo [A.6] Abuso de privilegios de acceso	[A.6] Abuso de privilegios de acceso	Improbable	Moderado	1	0,68	0,68	15	Baja
53	Acuerdos de software con terceros	Acuerdos de software con terceros	Acuerdos de software con terceros sobre	[I.5] Avería de origen físico o lógico	Improbable	Menor	1	0,5	0,5	11	Baja

N	Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Medición - Riesgo Inherente						
					Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
			el activo [I.5] Avería de origen físico o lógico								
54	Acuerdos de software con terceros	Acuerdos de software con terceros	Acuerdos de software con terceros sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja
55	Acuerdos de software con terceros	Acuerdos de software con terceros	Acuerdos de software con terceros sobre el activo [E.20] Vulnerabilidades de los programas (software)	[E.20] Vulnerabilidades de los programas (software)	Improbable	Menor	1	0,5	0,5	11	Baja
56	Acuerdos de software con terceros	Acuerdos de software con terceros	Acuerdos de software con terceros sobre el activo [A.6] Abuso de privilegios de acceso	[A.6] Abuso de privilegios de acceso	Improbable	Menor	1	0,5	0,5	11	Baja
57	Servidor servicios registrales	Servidor servicios registrales	Servidor servicios registrales sobre el activo [I.5] Avería de origen físico o lógico	[I.5] Avería de origen físico o lógico	Improbable	Menor	1	0,5	0,5	11	Baja
58	Servidor servicios registrales	Servidor servicios registrales	Servidor servicios registrales sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja
59	Servidor servicios registrales	Servidor servicios registrales	Servidor servicios registrales sobre el activo [E.20] Vulnerabilidades de los programas (software)	[E.20] Vulnerabilidades de los programas (software)	Improbable	Menor	1	0,5	0,5	11	Baja
60	Servidor servicios registrales	Servidor servicios registrales	Servidor servicios registrales sobre el activo [A.6] Abuso de privilegios de acceso	[A.6] Abuso de privilegios de acceso	Improbable	Menor	1	0,5	0,5	11	Baja
61	Servidor web servicios registrales	Servidor web servicios registrales	Servidor web servicios registrales sobre el activo [I.5] Avería de origen físico o lógico	[I.5] Avería de origen físico o lógico	Improbable	Menor	1	0,5	0,5	11	Baja

N	Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Medición - Riesgo Inherente						
					Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
62	Servidor web servicios registrales	Servidor web servicios registrales	Servidor web servicios registrales sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja
63	Servidor web servicios registrales	Servidor web servicios registrales	Servidor web servicios registrales sobre el activo [E.20] Vulnerabilidades de los programas (software)	[E.20] Vulnerabilidades de los programas (software)	Improbable	Menor	1	0,5	0,5	11	Baja
64	Servidor web servicios registrales	Servidor web servicios registrales	Servidor web servicios registrales sobre el activo [A.6] Abuso de privilegios de acceso	[A.6] Abuso de privilegios de acceso	Improbable	Menor	1	0,5	0,5	11	Baja
65	Servidor Web Registro Nacional de Turismo	Servidor Web Registro Nacional de Turismo	Servidor Web Registro Nacional de Turismo sobre el activo [I.5] Avería de origen físico o lógico	[I.5] Avería de origen físico o lógico	Improbable	Moderado	1	0,68	0,68	15	Baja
66	Servidor Web Registro Nacional de Turismo	Servidor Web Registro Nacional de Turismo	Servidor Web Registro Nacional de Turismo sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja
67	Servidor Web Registro Nacional de Turismo	Servidor Web Registro Nacional de Turismo	Servidor Web Registro Nacional de Turismo sobre el activo [E.20] Vulnerabilidades de los programas (software)	[E.20] Vulnerabilidades de los programas (software)	Improbable	Menor	1	0,5	0,5	11	Baja
68	Servidor Web Registro Nacional de Turismo	Servidor Web Registro Nacional de Turismo	Servidor Web Registro Nacional de Turismo sobre el activo [A.6] Abuso de privilegios de acceso	[A.6] Abuso de privilegios de acceso	Improbable	Menor	1	0,5	0,5	11	Baja
69	Servidor Crear empresa	Servidor Crear empresa	Servidor Crear empresa sobre el activo [I.5] Avería de origen físico o lógico	[I.5] Avería de origen físico o lógico	Improbable	Menor	1	0,5	0,5	11	Baja

N	Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Medición - Riesgo Inherente						
					Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
70	Servidor Crear empresa	Servidor Crear empresa	Servidor Crear empresa sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja
71	Servidor Crear empresa	Servidor Crear empresa	Servidor Crear empresa sobre el activo [E.20] Vulnerabilidades de los programas (software)	[E.20] Vulnerabilidades de los programas (software)	Improbable	Menor	1	0,5	0,5	11	Baja
72	Servidor Crear empresa	Servidor Crear empresa	Servidor Crear empresa sobre el activo [A.6] Abuso de privilegios de acceso	[A.6] Abuso de privilegios de acceso	Improbable	Menor	1	0,5	0,5	11	Baja
73	Outlook para conexión a servidor de correo interno	Outlook para conexión a servidor de correo interno	Outlook para conexión a servidor de correo interno sobre el activo [I.5] Avería de origen físico o lógico	[I.5] Avería de origen físico o lógico	Improbable	Menor	1	0,5	0,5	11	Baja
74	Outlook para conexión a servidor de correo interno	Outlook para conexión a servidor de correo interno	Outlook para conexión a servidor de correo interno sobre el activo [E.9] Errores de [re-]encaminamiento	[E.9] Errores de [re-]encaminamiento	Improbable	Menor	1	0,5	0,5	11	Baja
75	Outlook para conexión a servidor de correo interno	Outlook para conexión a servidor de correo interno	Outlook para conexión a servidor de correo interno sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja
76	Outlook para conexión a servidor de correo interno	Outlook para conexión a servidor de correo interno	Outlook para conexión a servidor de correo interno sobre el activo [E.9] Errores de [re-]encaminamiento	[E.9] Errores de [re-]encaminamiento	Improbable	Menor	1	0,5	0,5	11	Baja
77	Outlook para conexión a servidor de correo interno	Outlook para conexión a servidor de correo interno	Outlook para conexión a servidor de correo interno sobre el activo [E.20] Vulnerabilidades de los programas (software)	[E.20] Vulnerabilidades de los programas (software)	Improbable	Moderado	1	0,68	0,68	15	Baja

N	Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Medición - Riesgo Inherente						
					Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
78	Outlook para conexión a servidor de correo interno	Outlook para conexión a servidor de correo interno	Outlook para conexión a servidor de correo interno sobre el activo [A.6] Abuso de privilegios de acceso	[A.6] Abuso de privilegios de acceso	Improbable	Menor	1	0,5	0,5	11	Baja
79	Robot SMTP para aplicativos	Robot SMTP para aplicativos	Robot SMTP para aplicativos sobre el activo [I.5] Avería de origen físico o lógico	[I.5] Avería de origen físico o lógico	Improbable	Menor	1	0,5	0,5	11	Baja
80	Robot SMTP para aplicativos	Robot SMTP para aplicativos	Robot SMTP para aplicativos sobre el activo [E.9] Errores de [re-]encaminamiento	[E.9] Errores de [re-]encaminamiento	Improbable	Moderado	1	0,68	0,68	15	Baja
81	Robot SMTP para aplicativos	Robot SMTP para aplicativos	Robot SMTP para aplicativos sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja
82	Robot SMTP para aplicativos	Robot SMTP para aplicativos	Robot SMTP para aplicativos sobre el activo [E.20] Vulnerabilidades de los programas (software)	[E.20] Vulnerabilidades de los programas (software)	Improbable	Menor	1	0,5	0,5	11	Baja
83	Robot SMTP para aplicativos	Robot SMTP para aplicativos	Robot SMTP para aplicativos sobre el activo [A.6] Abuso de privilegios de acceso	[A.6] Abuso de privilegios de acceso	Improbable	Menor	1	0,5	0,5	11	Baja
84	Servicio de correo empresarial	Servicio de correo empresarial	Servicio de correo empresarial sobre el activo [I.5] Avería de origen físico o lógico	[I.5] Avería de origen físico o lógico	Improbable	Menor	1	0,5	0,5	11	Baja
85	Servicio de correo empresarial	Servicio de correo empresarial	Servicio de correo empresarial sobre el activo [E.8] Difusión de software dañino	[E.8] Difusión de software dañino	Improbable	Moderado	1	0,68	0,68	15	Baja
86	Servicio de correo empresarial	Servicio de correo empresarial	Servicio de correo empresarial sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja

N	Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Medición - Riesgo Inherente						
					Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
87	Servicio de correo empresarial	Servicio de correo empresarial	Servicio de correo empresarial sobre el activo [E.9] Errores de [re-]encaminamiento	[E.9] Errores de [re-]encaminamiento	Improbable	Menor	1	0,5	0,5	11	Baja
88	Servicio de correo empresarial	Servicio de correo empresarial	Servicio de correo empresarial sobre el activo [E.20] Vulnerabilidades de los programas (software)	[E.20] Vulnerabilidades de los programas (software)	Improbable	Menor	1	0,5	0,5	11	Baja
89	Servicio de correo empresarial	Servicio de correo empresarial	Servicio de correo empresarial sobre el activo [A.6] Abuso de privilegios de acceso	[A.6] Abuso de privilegios de acceso	Improbable	Menor	1	0,5	0,5	11	Baja
90	Navicat Gold	Navicat Gold	Navicat Gold sobre el activo [I.5] Avería de origen físico o lógico	[I.5] Avería de origen físico o lógico	Improbable	Menor	1	0,5	0,5	11	Baja
91	Navicat Gold	Navicat Gold	Navicat Gold sobre el activo [E.8] Difusión de software dañino	[E.8] Difusión de software dañino	Improbable	Menor	1	0,5	0,5	11	Baja
92	Navicat Gold	Navicat Gold	Navicat Gold sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja
93	Navicat Gold	Navicat Gold	Navicat Gold sobre el activo [E.20] Vulnerabilidades de los programas (software)	[E.20] Vulnerabilidades de los programas (software)	Improbable	Menor	1	0,5	0,5	11	Baja
94	Navicat Gold	Navicat Gold	Navicat Gold sobre el activo [A.6] Abuso de privilegios de acceso	[A.6] Abuso de privilegios de acceso	Improbable	Menor	1	0,5	0,5	11	Baja
95	Sistema Operativo Servidores	Sistema Operativo Servidores	Sistema Operativo Servidores sobre el activo [I.5] Avería de origen físico o lógico	[I.5] Avería de origen físico o lógico	Improbable	Menor	1	0,5	0,5	11	Baja
96	Sistema Operativo Servidores	Sistema Operativo Servidores	Sistema Operativo Servidores sobre el activo [E.2] Errores del	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja

N	Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Medición - Riesgo Inherente						
					Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
			administrador								
97	Sistema Operativo Servidores	Sistema Operativo Servidores	Sistema Operativo Servidores sobre el activo [E.20] Vulnerabilidades de los programas (software)	[E.20] Vulnerabilidades de los programas (software)	Poco Probable	Menor	1,3	0,5	0,65	14	Baja
98	Sistema Operativo Servidores	Sistema Operativo Servidores	Sistema Operativo Servidores sobre el activo [A.6] Abuso de privilegios de acceso	[A.6] Abuso de privilegios de acceso	Improbable	Moderado	1	0,68	0,68	15	Baja
99	Sistema Operativo funcionarios	Sistema Operativo funcionarios	Sistema Operativo funcionarios sobre el activo [I.5] Avería de origen físico o lógico	[I.5] Avería de origen físico o lógico	Improbable	Menor	1	0,5	0,5	11	Baja
100	Sistema Operativo funcionarios	Sistema Operativo funcionarios	Sistema Operativo funcionarios sobre el activo [E.8] Difusión de software dañino	[E.8] Difusión de software dañino	Improbable	Menor	1	0,5	0,5	11	Baja
101	Sistema Operativo funcionarios	Sistema Operativo funcionarios	Sistema Operativo funcionarios sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja
102	Sistema Operativo funcionarios	Sistema Operativo funcionarios	Sistema Operativo funcionarios sobre el activo [E.20] Vulnerabilidades de los programas (software)	[E.20] Vulnerabilidades de los programas (software)	Improbable	Menor	1	0,5	0,5	11	Baja
103	Sistema Operativo funcionarios	Sistema Operativo funcionarios	Sistema Operativo funcionarios sobre el activo [A.6] Abuso de privilegios de acceso	[A.6] Abuso de privilegios de acceso	Improbable	Menor	1	0,5	0,5	11	Baja
104	Sistema Operativo Soportes	Sistema Operativo Soportes	Sistema Operativo Soportes sobre el activo [I.5] Avería de origen físico o lógico	[I.5] Avería de origen físico o lógico	Improbable	Menor	1	0,5	0,5	11	Baja

N	Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Medición - Riesgo Inherente						
					Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
105	Sistema Operativo Soportes	Sistema Operativo Soportes	Sistema Operativo Soportes sobre el activo [E.8] Difusión de software dañino	[E.8] Difusión de software dañino	Improbable	Menor	1	0,5	0,5	11	Baja
106	Sistema Operativo Soportes	Sistema Operativo Soportes	Sistema Operativo Soportes sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja
107	Sistema Operativo Soportes	Sistema Operativo Soportes	Sistema Operativo Soportes sobre el activo [E.20] Vulnerabilidades de los programas (software)	[E.20] Vulnerabilidades de los programas (software)	Poco Probable	Menor	1,3	0,5	0,65	14	Baja
108	Sistema Operativo Soportes	Sistema Operativo Soportes	Sistema Operativo Soportes sobre el activo [A.6] Abuso de privilegios de acceso	[A.6] Abuso de privilegios de acceso	Improbable	Menor	1	0,5	0,5	11	Baja
109	Gestor plataforma de virtualización	Gestor plataforma de virtualización	Gestor plataforma de virtualización sobre el activo [I.5] Avería de origen físico o lógico	[I.5] Avería de origen físico o lógico	Improbable	Moderado	1	0,68	0,68	15	Baja
110	Gestor plataforma de virtualización	Gestor plataforma de virtualización	Gestor plataforma de virtualización sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Poco Probable	Menor	1,3	0,5	0,65	14	Baja
111	Gestor plataforma de virtualización	Gestor plataforma de virtualización	Gestor plataforma de virtualización sobre el activo [E.20] Vulnerabilidades de los programas (software)	[E.20] Vulnerabilidades de los programas (software)	Improbable	Menor	1	0,5	0,5	11	Baja
112	Gestor plataforma de virtualización	Gestor plataforma de virtualización	Gestor plataforma de virtualización sobre el activo [A.6] Abuso de privilegios de acceso	[A.6] Abuso de privilegios de acceso	Improbable	Menor	1	0,5	0,5	11	Baja
113	Host para solucion HA Vmware	Host para solucion HA Vmware	Host para solucion HA Vmware sobre el activo [N.1] Fuego	[N.1] Fuego	Improbable	Menor	1	0,5	0,5	11	Baja

N	Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Medición - Riesgo Inherente						
					Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
114	Host para solucion HA Vmware	Host para solucion HA Vmware	Host para solucion HA Vmware sobre el activo [N.*] Desastres naturales	[N.*] Desastres naturales	Improbable	Menor	1	0,5	0,5	11	Baja
115	Host para solucion HA Vmware	Host para solucion HA Vmware	Host para solucion HA Vmware sobre el activo [N.2] Daños por agua	[N.2] Daños por agua	Improbable	Menor	1	0,5	0,5	11	Baja
116	Host para solucion HA Vmware	Host para solucion HA Vmware	Host para solucion HA Vmware sobre el activo [I.3] Contaminación mecánica	[I.3] Contaminación mecánica	Improbable	Menor	1	0,5	0,5	11	Baja
117	Host para solucion HA Vmware	Host para solucion HA Vmware	Host para solucion HA Vmware sobre el activo [I.4] Contaminación electromagnética	[I.4] Contaminación electromagnética	Improbable	Menor	1	0,5	0,5	11	Baja
118	Host para solucion HA Vmware	Host para solucion HA Vmware	Host para solucion HA Vmware sobre el activo [I.5] Avería de origen físico o lógico	[I.5] Avería de origen físico o lógico	Improbable	Menor	1	0,5	0,5	11	Baja
119	Host para solucion HA Vmware	Host para solucion HA Vmware	Host para solucion HA Vmware sobre el activo [I.6] Corte del suministro eléctrico	[I.6] Corte del suministro eléctrico	Improbable	Menor	1	0,5	0,5	11	Baja
120	Host para solucion HA Vmware	Host para solucion HA Vmware	Host para solucion HA Vmware sobre el activo [I.7] Condiciones inadecuadas de Temperatura o humedad	[I.7] Condiciones inadecuadas de Temperatura o humedad	Improbable	Menor	1	0,5	0,5	11	Baja
121	Host para solucion HA Vmware	Host para solucion HA Vmware	Host para solucion HA Vmware sobre el activo [I.11] Emanaciones electromagnéticas	[I.11] Emanaciones electromagnéticas	Improbable	Menor	1	0,5	0,5	11	Baja
122	Host para solucion HA Vmware	Host para solucion HA Vmware	Host para solucion HA Vmware sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja
123	Servidor de desarrollo en Amazon	Servidor de desarrollo en Amazon	Servidor de desarrollo en Amazon sobre	[I.5] Avería de origen físico o lógico	Improbable	Menor	1	0,5	0,5	11	Baja

N	Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Medición - Riesgo Inherente						
					Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
			el activo [I.5] Avería de origen físico o lógico								
124	Servidor telefonia interna	Servidor telefonia interna	Servidor telefonia interna sobre el activo [N.1] Fuego	[N.1] Fuego	Improbable	Menor	1	0,5	0,5	11	Baja
125	Servidor telefonia interna	Servidor telefonia interna	Servidor telefonia interna sobre el activo [N.*] Desastres naturales	[N.*] Desastres naturales	Improbable	Menor	1	0,5	0,5	11	Baja
126	Servidor telefonia interna	Servidor telefonia interna	Servidor telefonia interna sobre el activo [N.2] Daños por agua	[N.2] Daños por agua	Improbable	Menor	1	0,5	0,5	11	Baja
127	Servidor telefonia interna	Servidor telefonia interna	Servidor telefonia interna sobre el activo [I.3] Contaminación mecánica	[I.3] Contaminación mecánica	Improbable	Menor	1	0,5	0,5	11	Baja
128	Servidor telefonia interna	Servidor telefonia interna	Servidor telefonia interna sobre el activo [I.4] Contaminación electromagnética	[I.4] Contaminación electromagnética	Improbable	Menor	1	0,5	0,5	11	Baja
129	Servidor telefonia interna	Servidor telefonia interna	Servidor telefonia interna sobre el activo [I.5] Avería de origen físico o lógico	[I.5] Avería de origen físico o lógico	Improbable	Menor	1	0,5	0,5	11	Baja
130	Servidor telefonia interna	Servidor telefonia interna	Servidor telefonia interna sobre el activo [I.6] Corte del suministro eléctrico	[I.6] Corte del suministro eléctrico	Improbable	Moderado	1	0,68	0,68	15	Baja
131	Servidor telefonia interna	Servidor telefonia interna	Servidor telefonia interna sobre el activo [I.7] Condiciones inadecuadas de temperatura o humedad	[I.7] Condiciones inadecuadas de temperatura o humedad	Improbable	Menor	1	0,5	0,5	11	Baja
132	Servidor telefonia interna	Servidor telefonia interna	Servidor telefonia interna sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Probable	Menor	1,35	0,5	0,675	15	Baja
133	Servidor de Correo OWA	Servidor de Correo OWA	Servidor de Correo OWA sobre el activo [I.5] Avería de origen físico o lógico	[I.5] Avería de origen físico o lógico	Improbable	Menor	1	0,5	0,5	11	Baja

N	Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Medición - Riesgo Inherente						
					Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
134	Servidor de Correo OWA	Servidor de Correo OWA	Servidor de Correo OWA sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja
135	Servidor servicios registrales	Servidor servicios registrales	Servidor servicios registrales sobre el activo [I.5] Avería de origen físico o lógico	[I.5] Avería de origen físico o lógico	Improbable	Menor	1	0,5	0,5	11	Baja
136	Servidor servicios registrales	Servidor servicios registrales	Servidor servicios registrales sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja
137	Servidor web servicios registrales	Servidor web servicios registrales	Servidor web servicios registrales sobre el activo [I.5] Avería de origen físico o lógico	[I.5] Avería de origen físico o lógico	Improbable	Menor	1	0,5	0,5	11	Baja
138	Servidor web servicios registrales	Servidor web servicios registrales	Servidor web servicios registrales sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja
139	Servidor Web Registro Nacional de Turismo	Servidor Web Registro Nacional de Turismo	Servidor Web Registro Nacional de Turismo sobre el activo [I.5] Avería de origen físico o lógico	[I.5] Avería de origen físico o lógico	Improbable	Menor	1	0,5	0,5	11	Baja
140	Servidor Web Registro Nacional de Turismo	Servidor Web Registro Nacional de Turismo	Servidor Web Registro Nacional de Turismo sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja
141	Servidor Crear empresa	Servidor Crear empresa	Servidor Crear empresa sobre el activo [I.5] Avería de origen físico o lógico	[I.5] Avería de origen físico o lógico	Improbable	Menor	1	0,5	0,5	11	Baja
142	Servidor Crear empresa	Servidor Crear empresa	Servidor Crear empresa sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja
143	Servidor de bases de datos	Servidor de bases de datos	Servidor de bases de datos sobre el activo [I.5] Avería de origen físico o	[I.5] Avería de origen físico o lógico	Improbable	Menor	1	0,5	0,5	11	Baja

N	Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Medición - Riesgo Inherente						
					Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
			lógico								
144	Servidor de bases de datos	Servidor de bases de datos	Servidor de bases de datos sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja
145	Servidor de Correo zimbra	Servidor de Correo zimbra	Servidor de Correo zimbra sobre el activo [I.5] Avería de origen físico o lógico	[I.5] Avería de origen físico o lógico	Improbable	Menor	1	0,5	0,5	11	Baja
146	Servidor de Correo zimbra	Servidor de Correo zimbra	Servidor de Correo zimbra sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja
147	Enrutador Red RUES	Enrutador Red RUES	Enrutador Red RUES sobre el activo [N.1] Fuego	[N.1] Fuego	Improbable	Menor	1	0,5	0,5	11	Baja
148	Enrutador Red RUES	Enrutador Red RUES	Enrutador Red RUES sobre el activo [N.*] Desastres naturales	[N.*] Desastres naturales	Improbable	Menor	1	0,5	0,5	11	Baja
149	Enrutador Red RUES	Enrutador Red RUES	Enrutador Red RUES sobre el activo [N.2] Daños por agua	[N.2] Daños por agua	Improbable	Menor	1	0,5	0,5	11	Baja
150	Enrutador Red RUES	Enrutador Red RUES	Enrutador Red RUES sobre el activo [I.3] Contaminación mecánica	[I.3] Contaminación mecánica	Improbable	Menor	1	0,5	0,5	11	Baja
151	Enrutador Red RUES	Enrutador Red RUES	Enrutador Red RUES sobre el activo [I.4] Contaminación electromagnética	[I.4] Contaminación electromagnética	Improbable	Menor	1	0,5	0,5	11	Baja
152	Enrutador Red RUES	Enrutador Red RUES	Enrutador Red RUES sobre el activo [I.5] Avería de origen físico o lógico	[I.5] Avería de origen físico o lógico	Improbable	Menor	1	0,5	0,5	11	Baja
153	Enrutador Red RUES	Enrutador Red RUES	Enrutador Red RUES sobre el activo [I.6] Corte del suministro eléctrico	[I.6] Corte del suministro eléctrico	Improbable	Menor	1	0,5	0,5	11	Baja
154	Enrutador Red RUES	Enrutador Red RUES	Enrutador Red RUES sobre el activo [I.7] Condiciones inadecuadas de temperatura o humedad	[I.7] Condiciones inadecuadas de temperatura o humedad	Improbable	Menor	1	0,5	0,5	11	Baja

N	Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Medición - Riesgo Inherente						
					Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
155	Enrutador Red RUES	Enrutador Red RUES	Enrutador Red RUES sobre el activo [I.11] Emanaciones electromagnéticas	[I.11] Emanaciones electromagnéticas	Improbable	Menor	1	0,5	0,5	11	Baja
156	Enrutador Red RUES	Enrutador Red RUES	Enrutador Red RUES sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja
157	Enrutador ISP Principal Synapsis	Enrutador ISP Principal Synapsis	Enrutador ISP Principal Synapsis sobre el activo [N.1] Fuego	[N.1] Fuego	Improbable	Menor	1	0,5	0,5	11	Baja
158	Enrutador ISP Principal Synapsis	Enrutador ISP Principal Synapsis	Enrutador ISP Principal Synapsis sobre el activo [N.*] Desastres naturales	[N.*] Desastres naturales	Improbable	Menor	1	0,5	0,5	11	Baja
159	Enrutador ISP Principal Synapsis	Enrutador ISP Principal Synapsis	Enrutador ISP Principal Synapsis sobre el activo [N.2] Daños por agua	[N.2] Daños por agua	Improbable	Menor	1	0,5	0,5	11	Baja
160	Enrutador ISP Principal Synapsis	Enrutador ISP Principal Synapsis	Enrutador ISP Principal Synapsis sobre el activo [I.3] Contaminación mecánica	[I.3] Contaminación mecánica	Improbable	Menor	1	0,5	0,5	11	Baja
161	Enrutador ISP Principal Synapsis	Enrutador ISP Principal Synapsis	Enrutador ISP Principal Synapsis sobre el activo [I.4] Contaminación electromagnética	[I.4] Contaminación electromagnética	Improbable	Menor	1	0,5	0,5	11	Baja
162	Enrutador ISP Principal Synapsis	Enrutador ISP Principal Synapsis	Enrutador ISP Principal Synapsis sobre el activo [I.5] Avería de origen físico o lógico	[I.5] Avería de origen físico o lógico	Improbable	Menor	1	0,5	0,5	11	Baja
163	Enrutador ISP Principal Synapsis	Enrutador ISP Principal Synapsis	Enrutador ISP Principal Synapsis sobre el activo [I.6] Corte del suministro eléctrico	[I.6] Corte del suministro eléctrico	Improbable	Menor	1	0,5	0,5	11	Baja
164	Enrutador ISP Principal Synapsis	Enrutador ISP Principal Synapsis	Enrutador ISP Principal Synapsis sobre el activo [I.7] Condiciones inadecuadas de temperatura o humedad	[I.7] Condiciones inadecuadas de temperatura o humedad	Improbable	Menor	1	0,5	0,5	11	Baja

N	Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Medición - Riesgo Inherente						
					Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
165	Enrutador ISP Principal Synapsis	Enrutador ISP Principal Synapsis	Enrutador ISP Principal Synapsis sobre el activo [I.11] Emanaciones electromagnéticas	[I.11] Emanaciones electromagnéticas	Improbable	Menor	1	0,5	0,5	11	Baja
166	Enrutador ISP Principal Synapsis	Enrutador ISP Principal Synapsis	Enrutador ISP Principal Synapsis sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja
167	Acceso internet contingencia	Acceso internet contingencia	Acceso internet contingencia sobre el activo [N.1] Fuego	[N.1] Fuego	Improbable	Menor	1	0,5	0,5	11	Baja
168	Acceso internet contingencia	Acceso internet contingencia	Acceso internet contingencia sobre el activo [N.*] Desastres naturales	[N.*] Desastres naturales	Improbable	Menor	1	0,5	0,5	11	Baja
169	Acceso internet contingencia	Acceso internet contingencia	Acceso internet contingencia sobre el activo [N.2] Daños por agua	[N.2] Daños por agua	Improbable	Menor	1	0,5	0,5	11	Baja
170	Acceso internet contingencia	Acceso internet contingencia	Acceso internet contingencia sobre el activo [I.3] Contaminación mecánica	[I.3] Contaminación mecánica	Improbable	Menor	1	0,5	0,5	11	Baja
171	Acceso internet contingencia	Acceso internet contingencia	Acceso internet contingencia sobre el activo [I.4] Contaminación electromagnética	[I.4] Contaminación electromagnética	Improbable	Menor	1	0,5	0,5	11	Baja
172	Acceso internet contingencia	Acceso internet contingencia	Acceso internet contingencia sobre el activo [I.5] Avería de origen físico o lógico	[I.5] Avería de origen físico o lógico	Improbable	Moderado	1	0,68	0,68	15	Baja
173	Acceso internet contingencia	Acceso internet contingencia	Acceso internet contingencia sobre el activo [I.6] Corte del suministro eléctrico	[I.6] Corte del suministro eléctrico	Improbable	Menor	1	0,5	0,5	11	Baja
174	Acceso internet contingencia	Acceso internet contingencia	Acceso internet contingencia sobre el activo [I.7] Condiciones inadecuadas de temperatura o humedad	[I.7] Condiciones inadecuadas de temperatura o humedad	Improbable	Menor	1	0,5	0,5	11	Baja

N	Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Medición - Riesgo Inherente						
					Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
175	Acceso internet contingencia	Acceso internet contingencia	Acceso internet contingencia sobre el activo [I.11] Emanaciones electromagnéticas	[I.11] Emanaciones electromagnéticas	Improbable	Menor	1	0,5	0,5	11	Baja
176	Acceso internet contingencia	Acceso internet contingencia	Acceso internet contingencia sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja
177	UTM Panorama	UTM Panorama	UTM Panorama sobre el activo [N.1] Fuego	[N.1] Fuego	Improbable	Menor	1	0,5	0,5	11	Baja
178	UTM Panorama	UTM Panorama	UTM Panorama sobre el activo [N.*] Desastres naturales	[N.*] Desastres naturales	Improbable	Menor	1	0,5	0,5	11	Baja
179	UTM Panorama	UTM Panorama	UTM Panorama sobre el activo [N.2] Daños por agua	[N.2] Daños por agua	Improbable	Menor	1	0,5	0,5	11	Baja
180	UTM Panorama	UTM Panorama	UTM Panorama sobre el activo [I.3] Contaminación mecánica	[I.3] Contaminación mecánica	Improbable	Menor	1	0,5	0,5	11	Baja
181	UTM Panorama	UTM Panorama	UTM Panorama sobre el activo [I.4] Contaminación electromagnética	[I.4] Contaminación electromagnética	Improbable	Menor	1	0,5	0,5	11	Baja
182	UTM Panorama	UTM Panorama	UTM Panorama sobre el activo [I.5] Avería de origen físico o lógico	[I.5] Avería de origen físico o lógico	Improbable	Menor	1	0,5	0,5	11	Baja
183	UTM Panorama	UTM Panorama	UTM Panorama sobre el activo [I.6] Corte del suministro eléctrico	[I.6] Corte del suministro eléctrico	Improbable	Menor	1	0,5	0,5	11	Baja
184	UTM Panorama	UTM Panorama	UTM Panorama sobre el activo [I.7] Condiciones inadecuadas de temperatura o humedad	[I.7] Condiciones inadecuadas de temperatura o humedad	Improbable	Menor	1	0,5	0,5	11	Baja
185	UTM Panorama	UTM Panorama	UTM Panorama sobre el activo [I.11] Emanaciones electromagnéticas	[I.11] Emanaciones electromagnéticas	Improbable	Menor	1	0,5	0,5	11	Baja
186	UTM Panorama	UTM Panorama	UTM Panorama sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja

N	Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Medición - Riesgo Inherente						
					Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
187	UTM Datacenter	UTM Datacenter	UTM Datacenter sobre el activo [N.1] Fuego	[N.1] Fuego	Improbable	Menor	1	0,5	0,5	11	Baja
188	UTM Datacenter	UTM Datacenter	UTM Datacenter sobre el activo [N.*] Desastres naturales	[N.*] Desastres naturales	Improbable	Menor	1	0,5	0,5	11	Baja
189	UTM Datacenter	UTM Datacenter	UTM Datacenter sobre el activo [N.2] Daños por agua	[N.2] Daños por agua	Improbable	Menor	1	0,5	0,5	11	Baja
190	UTM Datacenter	UTM Datacenter	UTM Datacenter sobre el activo [I.3] Contaminación mecánica	[I.3] Contaminación mecánica	Improbable	Menor	1	0,5	0,5	11	Baja
191	UTM Datacenter	UTM Datacenter	UTM Datacenter sobre el activo [I.4] Contaminación electromagnética	[I.4] Contaminación electromagnética	Improbable	Menor	1	0,5	0,5	11	Baja
192	UTM Datacenter	UTM Datacenter	UTM Datacenter sobre el activo [I.5] Avería de origen físico o lógico	[I.5] Avería de origen físico o lógico	Improbable	Menor	1	0,5	0,5	11	Baja
193	UTM Datacenter	UTM Datacenter	UTM Datacenter sobre el activo [I.6] Corte del suministro eléctrico	[I.6] Corte del suministro eléctrico	Improbable	Menor	1	0,5	0,5	11	Baja
194	UTM Datacenter	UTM Datacenter	UTM Datacenter sobre el activo [I.7] Condiciones inadecuadas de temperatura o humedad	[I.7] Condiciones inadecuadas de temperatura o humedad	Improbable	Menor	1	0,5	0,5	11	Baja
195	UTM Datacenter	UTM Datacenter	UTM Datacenter sobre el activo [I.11] Emanaciones electromagnéticas	[I.11] Emanaciones electromagnéticas	Improbable	Menor	1	0,5	0,5	11	Baja
196	UTM Datacenter	UTM Datacenter	UTM Datacenter sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja
197	Switch panorama LAN	Switch panorama LAN	Switch panorama LAN sobre el activo	[N.1] Fuego	Improbable	Menor	1	0,5	0,5	11	Baja

N	Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Medición - Riesgo Inherente						
					Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
			[N.1] Fuego								
198	Switch panorama LAN	Switch panorama LAN	Switch panorama LAN sobre el activo [N.*] Desastres naturales	[N.*] Desastres naturales	Improbable	Menor	1	0,5	0,5	11	Baja
199	Switch panorama LAN	Switch panorama LAN	Switch panorama LAN sobre el activo [N.2] Daños por agua	[N.2] Daños por agua	Improbable	Menor	1	0,5	0,5	11	Baja
200	Switch panorama LAN	Switch panorama LAN	Switch panorama LAN sobre el activo [I.3] Contaminación mecánica	[I.3] Contaminación mecánica	Improbable	Menor	1	0,5	0,5	11	Baja
201	Switch panorama LAN	Switch panorama LAN	Switch panorama LAN sobre el activo [I.4] Contaminación electromagnética	[I.4] Contaminación electromagnética	Improbable	Menor	1	0,5	0,5	11	Baja
202	Switch panorama LAN	Switch panorama LAN	Switch panorama LAN sobre el activo [I.5] Avería de origen físico o lógico	[I.5] Avería de origen físico o lógico	Improbable	Menor	1	0,5	0,5	11	Baja
203	Switch panorama LAN	Switch panorama LAN	Switch panorama LAN sobre el activo [I.6] Corte del suministro eléctrico	[I.6] Corte del suministro eléctrico	Improbable	Menor	1	0,5	0,5	11	Baja
204	Switch panorama LAN	Switch panorama LAN	Switch panorama LAN sobre el activo [I.7] Condiciones inadecuadas de temperatura o humedad	[I.7] Condiciones inadecuadas de temperatura o humedad	Improbable	Menor	1	0,5	0,5	11	Baja
205	Switch panorama LAN	Switch panorama LAN	Switch panorama LAN sobre el activo [I.11] Emanaciones electromagnéticas	[I.11] Emanaciones electromagnéticas	Improbable	Menor	1	0,5	0,5	11	Baja
206	Switch panorama LAN	Switch panorama LAN	Switch panorama LAN sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja
207	Switch panorama red RUES	Switch panorama red RUES	Switch panorama red RUES sobre el activo [N.1]	[N.1] Fuego	Improbable	Menor	1	0,5	0,5	11	Baja

N	Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Medición - Riesgo Inherente						
					Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
			Fuego								
208	Switch panorama red RUES	Switch panorama red RUES	Switch panorama red RUES sobre el activo [N.*] Desastres naturales	[N.*] Desastres naturales	Improbable	Menor	1	0,5	0,5	11	Baja
209	Switch panorama red RUES	Switch panorama red RUES	Switch panorama red RUES sobre el activo [N.2] Daños por agua	[N.2] Daños por agua	Improbable	Menor	1	0,5	0,5	11	Baja
210	Switch panorama red RUES	Switch panorama red RUES	Switch panorama red RUES sobre el activo [I.3] Contaminación mecánica	[I.3] Contaminación mecánica	Improbable	Menor	1	0,5	0,5	11	Baja
211	Switch panorama red RUES	Switch panorama red RUES	Switch panorama red RUES sobre el activo [I.4] Contaminación electromagnética	[I.4] Contaminación electromagnética	Improbable	Menor	1	0,5	0,5	11	Baja
212	Switch panorama red RUES	Switch panorama red RUES	Switch panorama red RUES sobre el activo [I.5] Avería de origen físico o lógico	[I.5] Avería de origen físico o lógico	Improbable	Menor	1	0,5	0,5	11	Baja
213	Switch panorama red RUES	Switch panorama red RUES	Switch panorama red RUES sobre el activo [I.6] Corte del suministro eléctrico	[I.6] Corte del suministro eléctrico	Improbable	Menor	1	0,5	0,5	11	Baja
214	Switch panorama red RUES	Switch panorama red RUES	Switch panorama red RUES sobre el activo [I.7] Condiciones inadecuadas de temperatura o humedad	[I.7] Condiciones inadecuadas de temperatura o humedad	Improbable	Menor	1	0,5	0,5	11	Baja
215	Switch panorama red RUES	Switch panorama red RUES	Switch panorama red RUES sobre el activo [I.11] Emanaciones electromagnéticas	[I.11] Emanaciones electromagnéticas	Improbable	Menor	1	0,5	0,5	11	Baja
216	Switch panorama red RUES	Switch panorama red RUES	Switch panorama red RUES sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja

N	Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Medición - Riesgo Inherente						
					Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
217	Switch Synapsis Lan	Switch Synapsis Lan	Switch Synapsis Lan sobre el activo [N.1] Fuego	[N.1] Fuego	Improbable	Menor	1	0,5	0,5	11	Baja
218	Switch Synapsis Lan	Switch Synapsis Lan	Switch Synapsis Lan sobre el activo [N.*] Desastres naturales	[N.*] Desastres naturales	Improbable	Menor	1	0,5	0,5	11	Baja
219	Switch Synapsis Lan	Switch Synapsis Lan	Switch Synapsis Lan sobre el activo [N.2] Daños por agua	[N.2] Daños por agua	Improbable	Menor	1	0,5	0,5	11	Baja
220	Switch Synapsis Lan	Switch Synapsis Lan	Switch Synapsis Lan sobre el activo [I.3] Contaminación mecánica	[I.3] Contaminación mecánica	Improbable	Menor	1	0,5	0,5	11	Baja
221	Switch Synapsis Lan	Switch Synapsis Lan	Switch Synapsis Lan sobre el activo [I.4] Contaminación electromagnética	[I.4] Contaminación electromagnética	Improbable	Menor	1	0,5	0,5	11	Baja
222	Switch Synapsis Lan	Switch Synapsis Lan	Switch Synapsis Lan sobre el activo [I.6] Corte del suministro eléctrico	[I.6] Corte del suministro eléctrico	Improbable	Menor	1	0,5	0,5	11	Baja
223	Switch Synapsis Lan	Switch Synapsis Lan	Switch Synapsis Lan sobre el activo [I.7] Condiciones inadecuadas de temperatura o humedad	[I.7] Condiciones inadecuadas de temperatura o humedad	Improbable	Menor	1	0,5	0,5	11	Baja
224	Switch Synapsis Lan	Switch Synapsis Lan	Switch Synapsis Lan sobre el activo [I.11] Emanaciones electromagnéticas	[I.11] Emanaciones electromagnéticas	Improbable	Menor	1	0,5	0,5	11	Baja
225	Switch Synapsis Lan	Switch Synapsis Lan	Switch Synapsis Lan sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja
226	Robot de Cintas	Robot de Cintas	Robot de Cintas sobre el activo [N.1] Fuego	[N.1] Fuego	Improbable	Menor	1	0,5	0,5	11	Baja
227	Robot de Cintas	Robot de Cintas	Robot de Cintas sobre el activo [N.*] Desastres naturales	[N.*] Desastres naturales	Improbable	Menor	1	0,5	0,5	11	Baja
228	Robot de Cintas	Robot de Cintas	Robot de Cintas sobre el activo [N.2] Daños por agua	[N.2] Daños por agua	Improbable	Menor	1	0,5	0,5	11	Baja
229	Robot de Cintas	Robot de Cintas	Robot de Cintas sobre el activo [I.3]	[I.3] Contaminación mecánica	Improbable	Menor	1	0,5	0,5	11	Baja

N	Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Medición - Riesgo Inherente						
					Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
			Contaminación mecánica								
230	Robot de Cintas	Robot de Cintas	Robot de Cintas sobre el activo [I.4] Contaminación electromagnética	[I.4] Contaminación electromagnética	Improbable	Menor	1	0,5	0,5	11	Baja
231	Robot de Cintas	Robot de Cintas	Robot de Cintas sobre el activo [I.6] Corte del suministro eléctrico	[I.6] Corte del suministro eléctrico	Improbable	Menor	1	0,5	0,5	11	Baja
232	Robot de Cintas	Robot de Cintas	Robot de Cintas sobre el activo [I.7] Condiciones inadecuadas de temperatura o humedad	[I.7] Condiciones inadecuadas de temperatura o humedad	Improbable	Menor	1	0,5	0,5	11	Baja
233	Robot de Cintas	Robot de Cintas	Robot de Cintas sobre el activo [I.11] Emanaciones electromagnéticas	[I.11] Emanaciones electromagnéticas	Improbable	Menor	1	0,5	0,5	11	Baja
234	Robot de Cintas	Robot de Cintas	Robot de Cintas sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja
235	sistemas de alimentación ininterrumpida	sistemas de alimentación ininterrumpida	sistemas de alimentación ininterrumpida sobre el activo [N.1] Fuego	[N.1] Fuego	Improbable	Menor	1	0,5	0,5	11	Baja
236	sistemas de alimentación ininterrumpida	sistemas de alimentación ininterrumpida	sistemas de alimentación ininterrumpida sobre el activo [N.*] Desastres naturales	[N.*] Desastres naturales	Improbable	Menor	1	0,5	0,5	11	Baja
237	sistemas de alimentación ininterrumpida	sistemas de alimentación ininterrumpida	sistemas de alimentación ininterrumpida sobre el activo [N.2] Daños por agua	[N.2] Daños por agua	Improbable	Menor	1	0,5	0,5	11	Baja
238	sistemas de alimentación ininterrumpida	sistemas de alimentación ininterrumpida	sistemas de alimentación ininterrumpida sobre el activo [I.3] Contaminación mecánica	[I.3] Contaminación mecánica	Improbable	Menor	1	0,5	0,5	11	Baja
239	sistemas de alimentación ininterrumpida	sistemas de alimentación ininterrumpida	sistemas de alimentación ininterrumpida sobre el activo [I.4] Contaminación electromagnética	[I.4] Contaminación electromagnética	Improbable	Menor	1	0,5	0,5	11	Baja

N	Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Medición - Riesgo Inherente						
					Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
			a								
240	sistemas de alimentación ininterrumpida	sistemas de alimentación ininterrumpida	sistemas de alimentación ininterrumpida sobre el activo [I.5] Avería de origen físico o lógico	[I.5] Avería de origen físico o lógico	Improbable	Menor	1	0,5	0,5	11	Baja
241	sistemas de alimentación ininterrumpida	sistemas de alimentación ininterrumpida	sistemas de alimentación ininterrumpida sobre el activo [I.6] Corte del suministro eléctrico	[I.6] Corte del suministro eléctrico	Improbable	Menor	1	0,5	0,5	11	Baja
242	sistemas de alimentación ininterrumpida	sistemas de alimentación ininterrumpida	sistemas de alimentación ininterrumpida sobre el activo [I.7] Condiciones inadecuadas de temperatura o humedad	[I.7] Condiciones inadecuadas de temperatura o humedad	Improbable	Menor	1	0,5	0,5	11	Baja
243	sistemas de alimentación ininterrumpida	sistemas de alimentación ininterrumpida	sistemas de alimentación ininterrumpida sobre el activo [I.9] Interrupción de otros servicios y suministros esenciales	[I.9] Interrupción de otros servicios y suministros esenciales	Improbable	Menor	1	0,5	0,5	11	Baja
244	sistemas de alimentación ininterrumpida	sistemas de alimentación ininterrumpida	sistemas de alimentación ininterrumpida sobre el activo [I.11] Emanaciones electromagnéticas	[I.11] Emanaciones electromagnéticas	Improbable	Menor	1	0,5	0,5	11	Baja
245	Almacenamiento en red	Almacenamiento en red	Almacenamiento en red sobre el activo [N.1] Fuego	[N.1] Fuego	Improbable	Menor	1	0,5	0,5	11	Baja
246	Almacenamiento en red	Almacenamiento en red	Almacenamiento en red sobre el activo [N.*] Desastres naturales	[N.*] Desastres naturales	Improbable	Menor	1	0,5	0,5	11	Baja
247	Almacenamiento en red	Almacenamiento en red	Almacenamiento en red sobre el activo [N.2] Daños por agua	[N.2] Daños por agua	Improbable	Menor	1	0,5	0,5	11	Baja
248	Almacenamiento en red	Almacenamiento en red	Almacenamiento en red sobre el activo [I.3] Contaminación mecánica	[I.3] Contaminación mecánica	Improbable	Menor	1	0,5	0,5	11	Baja

N	Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Medición - Riesgo Inherente						
					Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
249	Almacenamiento en red	Almacenamiento en red	Almacenamiento en red sobre el activo [I.4] Contaminación electromagnética	[I.4] Contaminación electromagnética	Improbable	Menor	1	0,5	0,5	11	Baja
250	Almacenamiento en red	Almacenamiento en red	Almacenamiento en red sobre el activo [I.6] Corte del suministro eléctrico	[I.6] Corte del suministro eléctrico	Improbable	Menor	1	0,5	0,5	11	Baja
251	Almacenamiento en red	Almacenamiento en red	Almacenamiento en red sobre el activo [I.7] Condiciones inadecuadas de temperatura o humedad	[I.7] Condiciones inadecuadas de temperatura o humedad	Improbable	Menor	1	0,5	0,5	11	Baja
252	Almacenamiento en red	Almacenamiento en red	Almacenamiento en red sobre el activo [I.10] Degradación de los soportes de almacenamiento de la información	[I.10] Degradación de los soportes de almacenamiento de la información	Improbable	Menor	1	0,5	0,5	11	Baja
253	Almacenamiento en red	Almacenamiento en red	Almacenamiento en red sobre el activo [I.11] Emanaciones electromagnéticas	[I.11] Emanaciones electromagnéticas	Improbable	Menor	1	0,5	0,5	11	Baja
254	Almacenamiento en red	Almacenamiento en red	Almacenamiento en red sobre el activo [E.2] Errores del administrador	[E.2] Errores del administrador	Improbable	Menor	1	0,5	0,5	11	Baja
255	Wifi contingencia y navegacion libre	Wifi contingencia y navegacion libre	Wifi contingencia y navegacion libre sobre el activo [I.8] Fallo de servicios de comunicaciones	[I.8] Fallo de servicios de comunicaciones	Improbable	Menor	1	0,5	0,5	11	Baja
256	Wifi contingencia y navegacion libre	Wifi contingencia y navegacion libre	Wifi contingencia y navegacion libre sobre el activo [A.6] Abuso de privilegios de acceso	[A.6] Abuso de privilegios de acceso	Improbable	Menor	1	0,5	0,5	11	Baja
257	Red corporativa de voz y datos	Red corporativa de voz y datos	Red corporativa de voz y datos sobre el activo [I.8] Fallo de servicios de comunicaciones	[I.8] Fallo de servicios de comunicaciones	Muy Frecuente	Mayor	1,5	0,77	1,155	48	Alta
258	Red corporativa de voz y datos	Red corporativa de voz y datos	Red corporativa de voz y datos sobre el activo [A.6] Abuso de	[A.6] Abuso de privilegios de acceso	Improbable	Menor	1	0,5	0,5	11	Baja

N	Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Medición - Riesgo Inherente						
					Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
			privilegios de acceso								
259	Red Datacenter RUES	Red Datacenter RUES	Red Datacenter RUES sobre el activo [I.8] Fallo de servicios de comunicaciones	[I.8] Fallo de servicios de comunicaciones	Muy Frecuente	Severo	1,5	0,8	1,2	50	Alta
260	Red Datacenter RUES	Red Datacenter RUES	Red Datacenter RUES sobre el activo [A.6] Abuso de privilegios de acceso	[A.6] Abuso de privilegios de acceso	Improbable	Menor	1	0,5	0,5	11	Baja
261	Red LAN Datacenter	Red LAN Datacenter	Red LAN Datacenter sobre el activo [I.8] Fallo de servicios de comunicaciones	[I.8] Fallo de servicios de comunicaciones	Muy Frecuente	Severo	1,5	0,8	1,2	50	Alta
262	Red LAN Datacenter	Red LAN Datacenter	Red LAN Datacenter sobre el activo [A.6] Abuso de privilegios de acceso	[A.6] Abuso de privilegios de acceso	Improbable	Menor	1	0,5	0,5	11	Baja
263	Red de internet principal	Red de internet principal	Red de internet principal sobre el activo [I.8] Fallo de servicios de comunicaciones	[I.8] Fallo de servicios de comunicaciones	Muy Frecuente	Severo	1,5	0,8	1,2	50	Alta
264	Red de internet principal	Red de internet principal	Red de internet principal sobre el activo [A.6] Abuso de privilegios de acceso	[A.6] Abuso de privilegios de acceso	Improbable	Menor	1	0,5	0,5	11	Baja
265	Red de navegación privada interconexión nacional Cámaras de Comercio	Red de navegacion privada interconexion nacional Camaras de Comercio	Red de navegacion privada interconexion nacional Camaras de Comercio sobre el activo [I.8] Fallo de servicios de comunicaciones	[I.8] Fallo de servicios de comunicaciones	Probable	Mayor	1,35	0,77	1,0395	43	Alta
266	Red de navegacion privada interconexion nacional Camaras de Comercio	Red de navegacion privada interconexion nacional Camaras de Comercio	Red de navegacion privada interconexion nacional Camaras de Comercio sobre el activo [A.6] Abuso de privilegios de acceso	[A.6] Abuso de privilegios de acceso	Improbable	Menor	1	0,5	0,5	11	Baja
267	Edificio panorama	Edificio panorama	Edificio panorama	[N.1] Fuego	Improbable	Menor	1	0,5	0,5	11	Baja

N	Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Medición - Riesgo Inherente						
					Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
	principal	principal	principal sobre el activo [N.1] Fuego								
268	Edificio panorama principal	Edificio panorama principal	Edificio panorama principal sobre el activo [N.*] Desastres naturales	[N.*] Desastres naturales	Improbable	Menor	1	0,5	0,5	11	Baja
269	Edificio panorama principal	Edificio panorama principal	Edificio panorama principal sobre el activo [N.2] Daños por agua	[N.2] Daños por agua	Improbable	Menor	1	0,5	0,5	11	Baja
270	Edificio panorama principal	Edificio panorama principal	Edificio panorama principal sobre el activo [I.3] Contaminación mecánica	[I.3] Contaminación mecánica	Improbable	Menor	1	0,5	0,5	11	Baja
271	Edificio panorama principal	Edificio panorama principal	Edificio panorama principal sobre el activo [I.11] Emanaciones electromagnéticas	[I.11] Emanaciones electromagnéticas	Improbable	Menor	1	0,5	0,5	11	Baja
272	Edificio datacenter ZonaFranca Synapsis	Edificio datacenter ZonaFranca Synapsis	Edificio datacenter ZonaFranca Synapsis sobre el activo [N.1] Fuego	[N.1] Fuego	Improbable	Menor	1	0,5	0,5	11	Baja
273	Edificio datacenter ZonaFranca Synapsis	Edificio datacenter ZonaFranca Synapsis	Edificio datacenter ZonaFranca Synapsis sobre el activo [N.*] Desastres naturales	[N.*] Desastres naturales	Improbable	Menor	1	0,5	0,5	11	Baja
274	Edificio datacenter ZonaFranca Synapsis	Edificio datacenter ZonaFranca Synapsis	Edificio datacenter ZonaFranca Synapsis sobre el activo [N.2] Daños por agua	[N.2] Daños por agua	Improbable	Menor	1	0,5	0,5	11	Baja
275	Edificio datacenter ZonaFranca Synapsis	Edificio datacenter ZonaFranca Synapsis	Edificio datacenter ZonaFranca Synapsis sobre el activo [I.3] Contaminación mecánica	[I.3] Contaminación mecánica	Improbable	Menor	1	0,5	0,5	11	Baja
276	Edificio datacenter ZonaFranca Synapsis	Edificio datacenter ZonaFranca Synapsis	Edificio datacenter ZonaFranca Synapsis sobre el activo [I.11] Emanaciones electromagnéticas	[I.11] Emanaciones electromagnéticas	Improbable	Menor	1	0,5	0,5	11	Baja

N	Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Medición - Riesgo Inherente						
					Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
277	Usuarios de atención al cliente i E y administrativos de todas las jerarquías	Usuarios de atencion al cliente i E y administrativos de todas las jerarquias	Usuarios de atencion al cliente i E y administrativos de todas las jerarquias sobre el activo [E.7] Deficiencias en la organización	[E.7] Deficiencias en la organización	Improbable	Menor	1	0,5	0,5	11	Baja
278	Usuarios de atencion al cliente i E y administrativos de todas las jerarquias	Usuarios de atencion al cliente i E y administrativos de todas las jerarquias	Usuarios de atencion al cliente i E y administrativos de todas las jerarquias sobre el activo [A.28] Indisponibilidad del personal	[A.28] Indisponibilidad del personal	Improbable	Menor	1	0,5	0,5	11	Baja
279	Usuarios de atencion al cliente i E y administrativos de todas las jerarquias	Usuarios de atencion al cliente i E y administrativos de todas las jerarquias	Usuarios de atencion al cliente i E y administrativos de todas las jerarquias sobre el activo [A.30] Ingeniería social (picaresca)	[A.30] Ingeniería social (picaresca)	Improbable	Menor	1	0,5	0,5	11	Baja
280	Administrador de infraestructura	Administrador de infraestructura	Administrador de infraestructura sobre el activo [E.7] Deficiencias en la organización	[E.7] Deficiencias en la organización	Probable	Mayor	1,35	0,77	1,0395	43	Alta
281	Administrador de infraestructura	Administrador de infraestructura	Administrador de infraestructura sobre el activo [A.28] Indisponibilidad del personal	[A.28] Indisponibilidad del personal	Improbable	Menor	1	0,5	0,5	11	Baja
282	Administrador de infraestructura	Administrador de infraestructura	Administrador de infraestructura sobre el activo [A.30] Ingeniería social (picaresca)	[A.30] Ingeniería social (picaresca)	Improbable	Menor	1	0,5	0,5	11	Baja
283	Equipo de desarrollo y soporte	Equipo de desarrollo y soporte	Equipo de desarrollo y soporte sobre el activo [E.7] Deficiencias en la organización	[E.7] Deficiencias en la organización	Probable	Mayor	1,35	0,77	1,0395	43	Alta
284	Equipo de desarrollo y soporte	Equipo de desarrollo y soporte	Equipo de desarrollo y soporte sobre el activo [A.28] Indisponibilidad del personal	[A.28] Indisponibilidad del personal	Improbable	Menor	1	0,5	0,5	11	Baja

N	Servicio	Nombre Servidor / Máquina Virtual / Activo	Descripción	Evento de Riesgo	Medición - Riesgo Inherente						
					Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
285	Equipo de desarrollo y soporte	Equipo de desarrollo y soporte	Equipo de desarrollo y soporte sobre el activo [A.30] Ingeniería social (picaresca)	[A.30] Ingeniería social (picaresca)	Improbable	Menor	1	0,5	0,5	11	Baja

MATRIZ DE RIESGOS DEL SGSI - RIESGO INHERENTE

N	Control para Frecuencia	Control para Impacto	Medición - Riesgo Residual						
			Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
1	Control de acceso lógico	Verificación de las funciones de seguridad	Improbable	Menor	1	0,5	0,5	11	Baja
2	Control de acceso lógico	Control de acceso lógico	Poco Probable	Menor	1,3	0,5	0,65	27	Media
3	Activación y/o Reconfiguración del servicio	Verificación de las funciones de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
4	Verificación de las funciones de seguridad	Verificación de las funciones de seguridad	Improbable	Moderado	1	0,68	0,68	28	Media
5	Verificación de las funciones de seguridad	Verificación de las funciones de seguridad	Probable	Menor	1,35	0,5	0,675	28	Media
6	Control de acceso lógico	Control de acceso lógico	Improbable	Menor	1	0,5	0,5	21	Media
7	Control de acceso lógico	Control de acceso lógico	Improbable	Menor	1	0,5	0,5	21	Media
8	Herramienta contra código dañino	Verificación de las funciones de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
9	Copias de seguridad de los datos (backup)	Copias de seguridad de los datos (backup)	Improbable	Menor	1	0,5	0,5	21	Media
10	Herramienta contra código dañino	Herramienta contra código dañino	Improbable	Menor	1	0,5	0,5	21	Media
11	Copias de seguridad de los datos (backup)	Copias de seguridad de los datos (backup)	Improbable	Menor	1	0,5	0,5	21	Media
12	Herramienta contra código dañino	Herramienta contra código dañino	Poco Probable	Moderado	1,3	0,68	0,884	37	Alta
13	Copias de seguridad de los datos (backup)	Verificación de las funciones de seguridad	Improbable	Moderado	1	0,68	0,68	28	Media

N	Control para Frecuencia	Control para Impacto	Medición - Riesgo Residual						
			Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
14	Herramienta contra código dañino	Verificación de las funciones de seguridad	Poco Probable	Menor	1,3	0,5	0,65	27	Media
15	Herramienta contra código dañino	Aseguramiento de la disponibilidad	Improbable	Menor	1	0,5	0,5	21	Media
16	Copias de seguridad de los datos (backup)	Aceptación y puesta en operación	Improbable	Menor	1	0,5	0,5	21	Media
17	Herramienta contra código dañino	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
18	Copias de seguridad de los datos (backup)	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
19	Cifrado de la información	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
20	Control de acceso lógico	Cambios (actualizaciones y mantenimiento)	Improbable	Menor	1	0,5	0,5	21	Media
21	Copias de seguridad de los datos (backup)	Copias de seguridad (backup)	Poco Probable	Menor	1,3	0,5	0,65	27	Media
22	Control de acceso lógico	Puesta en producción	Improbable	Moderado	1	0,68	0,68	28	Media
23	Copias de seguridad de los datos (backup)	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
24	Gestión de claves de firma de información	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
25	Control de acceso lógico	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media

N	Control para Frecuencia	Control para Impacto	Medición - Riesgo Residual						
			Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
26	Control de acceso lógico	Se aplican perfiles de seguridad	Poco Probable	Menor	1,3	0,5	0,65	27	Media
27	Verificación de las funciones de seguridad	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
28	Verificación de las funciones de seguridad	Puesta en producción	Improbable	Moderado	1	0,68	0,68	28	Media
29	Control de acceso lógico	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
30	Control de acceso lógico	Copias de seguridad (backup)	Poco Probable	Menor	1,3	0,5	0,65	27	Media
31	Herramienta contra código dañino	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
32	Copias de seguridad de los datos (backup)	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
33	Herramienta contra código dañino	Aseguramiento de la disponibilidad	Improbable	Menor	1	0,5	0,5	21	Media
34	Copias de seguridad de los datos (backup)	Aceptación y puesta en operación	Improbable	Moderado	1	0,68	0,68	28	Media
35	Herramienta contra código dañino	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
36	Copias de seguridad de los datos (backup)	Copias de seguridad (backup)	Poco Probable	Menor	1,3	0,5	0,65	27	Media
37	Herramienta contra código dañino	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
38	Copias de seguridad de los datos (backup)	Cambios (actualizaciones y mantenimiento)	Improbable	Menor	1	0,5	0,5	21	Media
39	Cifrado de la información	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
40	Control de acceso lógico	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media

N	Control para Frecuencia	Control para Impacto	Medición - Riesgo Residual						
			Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
41	Copias de seguridad de los datos (backup)	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
42	Control de acceso lógico	Copias de seguridad (backup)	Improbable	Moderado	1	0,68	0,68	28	Media
43	Copias de seguridad de los datos (backup)	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
44	Gestión de claves de firma de información	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
45	Gestión de claves de firma de información	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
46	Aseguramiento de la disponibilidad	Puesta en producción	Poco Probable	Menor	1,3	0,5	0,65	27	Media
47	Aceptación y puesta en operación	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
48	Aseguramiento de la disponibilidad	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
49	Aceptación y puesta en operación	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
50	Aseguramiento de la disponibilidad	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
51	Aceptación y puesta en operación	Aseguramiento de la disponibilidad	Improbable	Menor	1	0,5	0,5	21	Media
52	Aseguramiento de la disponibilidad	Aceptación y puesta en operación	Improbable	Moderado	1	0,68	0,68	28	Media
53	Aceptación y puesta en operación	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
54	Aseguramiento de la disponibilidad	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media

N	Control para Frecuencia	Control para Impacto	Medición - Riesgo Residual						
			Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
55	Aceptación y puesta en operación	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
56	Protección del correo electrónico	Cambios (actualizaciones y mantenimiento)	Improbable	Menor	1	0,5	0,5	21	Media
57	Aseguramiento de la disponibilidad	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
58	Aceptación y puesta en operación	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
59	Aseguramiento de la disponibilidad	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
60	Aceptación y puesta en operación	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
61	Aseguramiento de la disponibilidad	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
62	Aceptación y puesta en operación	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
63	Aseguramiento de la disponibilidad	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
64	Aceptación y puesta en operación	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
65	Aseguramiento de la disponibilidad	Se aplican perfiles de seguridad	Improbable	Moderado	1	0,68	0,68	28	Media
66	Aceptación y puesta en operación	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
67	Aseguramiento de la disponibilidad	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
68	Aceptación y puesta en operación	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
69	Copias de seguridad (backup)	Aseguramiento de la disponibilidad	Improbable	Menor	1	0,5	0,5	21	Media
70	Copias de seguridad (backup)	Aceptación y puesta en operación	Improbable	Menor	1	0,5	0,5	21	Media
71	Copias de seguridad (backup)	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
72	Cambios (actualizaciones y mantenimiento)	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media

N	Control para Frecuencia	Control para Impacto	Medición - Riesgo Residual						
			Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
73	Copias de seguridad (backup)	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
74	Puesta en producción	Cambios (actualizaciones y mantenimiento)	Improbable	Menor	1	0,5	0,5	21	Media
75	Se aplican perfiles de seguridad	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
76	Copias de seguridad (backup)	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
77	Puesta en producción	Se aplican perfiles de seguridad	Improbable	Moderado	1	0,68	0,68	28	Media
78	Se aplican perfiles de seguridad	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
79	Copias de seguridad (backup)	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
80	Puesta en producción	Se aplican perfiles de seguridad	Improbable	Moderado	1	0,68	0,68	28	Media
81	Se aplican perfiles de seguridad	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
82	Copias de seguridad (backup)	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
83	Puesta en producción	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
84	Se aplican perfiles de seguridad	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
85	Copias de seguridad (backup)	Puesta en producción	Improbable	Moderado	1	0,68	0,68	28	Media
86	Copias de seguridad (backup)	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
87	Copias de seguridad (backup)	Aseguramiento de la disponibilidad	Improbable	Menor	1	0,5	0,5	21	Media
88	Copias de seguridad (backup)	Aceptación y puesta en operación	Improbable	Menor	1	0,5	0,5	21	Media
89	Copias de seguridad (backup)	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
90	Copias de seguridad (backup)	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
91	Copias de seguridad (backup)	Copias de	Improbable	Menor	1	0,5	0,5	21	Media

N	Control para Frecuencia	Control para Impacto	Medición - Riesgo Residual						
			Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
		seguridad (backup)							
92	Copias de seguridad (backup)	Cambios (actualizaciones y mantenimiento)	Improbable	Menor	1	0,5	0,5	21	Media
93	Copias de seguridad (backup)	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
94	Copias de seguridad (backup)	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
95	Aseguramiento de la disponibilidad	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
96		Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
97	Protección de los Equipos Informáticos	Puesta en producción	Poco Probable	Menor	1,3	0,5	0,65	27	Media
98		Se aplican perfiles de seguridad	Improbable	Moderado	1	0,68	0,68	28	Media
99		Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
100		Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
101		Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
102	Operación	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
103	Protección de los Equipos Informáticos	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
104	Protección de los Equipos Informáticos	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
105	Protección de los Equipos Informáticos	Aseguramiento de la disponibilidad	Improbable	Menor	1	0,5	0,5	21	Media
106	Se aplican perfiles de seguridad	Aceptación y puesta en operación	Improbable	Menor	1	0,5	0,5	21	Media
107	Se aplican perfiles de seguridad	Copias de seguridad (backup)	Poco Probable	Menor	1,3	0,5	0,65	27	Media
108	Se aplican perfiles de seguridad	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
109	Se aplican perfiles de seguridad	Copias de seguridad (backup)	Improbable	Moderado	1	0,68	0,68	28	Media
110	Se aplican perfiles de seguridad	Cambios (actualizaciones y mantenimiento)	Poco Probable	Menor	1,3	0,5	0,65	27	Media

N	Control para Frecuencia	Control para Impacto	Medición - Riesgo Residual						
			Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
111	Se aplican perfiles de seguridad	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
112	Protección de los Equipos Informáticos	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
113	Protección de los Equipos Informáticos	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
114	Protección de los Equipos Informáticos	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
115	Protección de los Equipos Informáticos	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
116	Protección de los Equipos Informáticos	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
117	Protección de los Equipos Informáticos	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
118	Protección de los Equipos Informáticos	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
119	Protección de los Equipos Informáticos	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
120	Protección de los Equipos Informáticos	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
121	Protección de los Equipos Informáticos	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
122	Aseguramiento de la disponibilidad	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
123	Protección de los Equipos Informáticos	Aseguramiento de la disponibilidad	Improbable	Menor	1	0,5	0,5	21	Media
124	Protección de los Equipos Informáticos	Aceptación y puesta en operación	Improbable	Menor	1	0,5	0,5	21	Media
125	Protección de los Equipos Informáticos	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
126	Seguridad Wireless (WiFi)	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
127	Aseguramiento de la disponibilidad	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
128	Aseguramiento de la disponibilidad	Cambios (actualizaciones y mantenimiento)	Improbable	Menor	1	0,5	0,5	21	Media
129	Aseguramiento de la disponibilidad	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media

N	Control para Frecuencia	Control para Impacto	Medición - Riesgo Residual						
			Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
130	Aseguramiento de la disponibilidad	Puesta en producción	Improbable	Moderado	1	0,68	0,68	28	Media
131	Se aplican perfiles de seguridad	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
132	Operación	Copias de seguridad (backup)	Probable	Menor	1,35	0,5	0,675	28	Media
133	Segregación de las redes en dominios	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
134	Sistema de protección perimetral	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
135	Aseguramiento de la disponibilidad	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
136	Diseño	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
137	Control de los accesos físicos	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
138	Diseño	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
139	Defensa en profundidad	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
140	Control de los accesos físicos	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
141	Aseguramiento de la disponibilidad	Aseguramiento de la disponibilidad	Improbable	Menor	1	0,5	0,5	21	Media
142	Plan de Recuperación de Desastres (DRP)	Aceptación y puesta en operación	Improbable	Menor	1	0,5	0,5	21	Media
143	Formación y concienciación	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
144	Aseguramiento de la disponibilidad	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
145	Formación y concienciación	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
146	Aseguramiento de la disponibilidad	Cambios (actualizaciones y mantenimiento)	Improbable	Menor	1	0,5	0,5	21	Media
147	Formación y concienciación	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
148	Aseguramiento de la disponibilidad	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
149	Control de acceso lógico	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
150	Control de acceso lógico	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media

N	Control para Frecuencia	Control para Impacto	Medición - Riesgo Residual						
			Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
151	Verificación de las funciones de seguridad	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
152	Verificación de las funciones de seguridad	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
153	Control de acceso lógico	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
154	Control de acceso lógico	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
155	Herramienta contra código dañino	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
156	Copias de seguridad de los datos (backup)	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
157	Herramienta contra código dañino	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
158	Copias de seguridad de los datos (backup)	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
159	Herramienta contra código dañino	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
160	Copias de seguridad de los datos (backup)	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
161	Herramienta contra código dañino	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
162	Copias de seguridad de los datos (backup)	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
163	Cifrado de la información	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
164	Control de acceso lógico	Aseguramiento de la disponibilidad	Improbable	Menor	1	0,5	0,5	21	Media
165	Copias de seguridad de los datos (backup)	Aceptación y puesta en operación	Improbable	Menor	1	0,5	0,5	21	Media
166	Control de acceso lógico	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
167	Copias de seguridad de los datos (backup)	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
168	Gestión de claves de firma de información	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
169	Gestión de claves de firma de información	Cambios (actualizaciones y mantenimiento)	Improbable	Menor	1	0,5	0,5	21	Media
170	Aseguramiento de la disponibilidad	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
171	Aceptación y puesta en operación	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media

N	Control para Frecuencia	Control para Impacto	Medición - Riesgo Residual						
			Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
172	Aseguramiento de la disponibilidad	Se aplican perfiles de seguridad	Improbable	Moderado	1	0,68	0,68	28	Media
173	Aceptación y puesta en operación	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
174	Aseguramiento de la disponibilidad	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
175	Aceptación y puesta en operación	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
176	Aseguramiento de la disponibilidad	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
177	Aceptación y puesta en operación	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
178	Aseguramiento de la disponibilidad	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
179	Aceptación y puesta en operación	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
180	Protección del correo electrónico	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
181	Aseguramiento de la disponibilidad	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
182	Aceptación y puesta en operación	Aseguramiento de la disponibilidad	Improbable	Menor	1	0,5	0,5	21	Media
183	Aseguramiento de la disponibilidad	Aceptación y puesta en operación	Improbable	Menor	1	0,5	0,5	21	Media
184	Aceptación y puesta en operación	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
185	Aseguramiento de la disponibilidad	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
186	Aceptación y puesta en operación	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
187	Aseguramiento de la disponibilidad	Cambios (actualizaciones y mantenimiento)	Improbable	Menor	1	0,5	0,5	21	Media
188	Aceptación y puesta en operación	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
189	Aseguramiento de la disponibilidad	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
190	Aceptación y puesta en operación	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
191	Aseguramiento de la disponibilidad	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
192	Aceptación y puesta en operación	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media

N	Control para Frecuencia	Control para Impacto	Medición - Riesgo Residual						
			Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
193	Copias de seguridad (backup)	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
194	Copias de seguridad (backup)	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
195	Copias de seguridad (backup)	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
196	Cambios (actualizaciones y mantenimiento)	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
197	Copias de seguridad (backup)	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
198	Puesta en producción	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
199	Se aplican perfiles de seguridad	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
200	Copias de seguridad (backup)	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
201	Puesta en producción	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
202	Se aplican perfiles de seguridad	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
203	Copias de seguridad (backup)	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
204	Puesta en producción	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
205	Se aplican perfiles de seguridad	Aseguramiento de la disponibilidad	Improbable	Menor	1	0,5	0,5	21	Media
206	Copias de seguridad (backup)	Aceptación y puesta en operación	Improbable	Menor	1	0,5	0,5	21	Media
207	Puesta en producción	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
208	Se aplican perfiles de seguridad	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
209	Copias de seguridad (backup)	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
210	Copias de seguridad (backup)	Cambios (actualizaciones y mantenimiento)	Improbable	Menor	1	0,5	0,5	21	Media
211	Copias de seguridad (backup)	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
212	Copias de seguridad (backup)	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
213	Copias de seguridad (backup)	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media

N	Control para Frecuencia	Control para Impacto	Medición - Riesgo Residual						
			Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
214	Copias de seguridad (backup)	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
215	Copias de seguridad (backup)	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
216	Copias de seguridad (backup)	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
217	Copias de seguridad (backup)	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
218	Copias de seguridad (backup)	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
219	Aseguramiento de la disponibilidad	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
220		Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
221	Protección de los Equipos Informáticos	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
222		Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
223		Aseguramiento de la disponibilidad	Improbable	Menor	1	0,5	0,5	21	Media
224		Aceptación y puesta en operación	Improbable	Menor	1	0,5	0,5	21	Media
225		Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
226	Operación	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
227	Protección de los Equipos Informáticos	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
228	Protección de los Equipos Informáticos	Cambios (actualizaciones y mantenimiento)	Improbable	Menor	1	0,5	0,5	21	Media
229	Protección de los Equipos Informáticos	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
230	Se aplican perfiles de seguridad	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
231	Se aplican perfiles de seguridad	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
232	Se aplican perfiles de seguridad	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
233	Se aplican perfiles de seguridad	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
234	Se aplican perfiles de seguridad	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media

N	Control para Frecuencia	Control para Impacto	Medición - Riesgo Residual						
			Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
235	Se aplican perfiles de seguridad	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
236	Protección de los Equipos Informáticos	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
237	Protección de los Equipos Informáticos	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
238	Protección de los Equipos Informáticos	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
239	Protección de los Equipos Informáticos	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
240	Protección de los Equipos Informáticos	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
241	Protección de los Equipos Informáticos	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
242	Protección de los Equipos Informáticos	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
243	Protección de los Equipos Informáticos	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
244	Protección de los Equipos Informáticos	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
245	Protección de los Equipos Informáticos	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
246	Aseguramiento de la disponibilidad	Aseguramiento de la disponibilidad	Improbable	Menor	1	0,5	0,5	21	Media
247	Protección de los Equipos Informáticos	Aceptación y puesta en operación	Improbable	Menor	1	0,5	0,5	21	Media
248	Protección de los Equipos Informáticos	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
249	Protección de los Equipos Informáticos	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
250	Seguridad Wireless (WiFi)	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
251	Aseguramiento de la disponibilidad	Cambios (actualizaciones y mantenimiento)	Improbable	Menor	1	0,5	0,5	21	Media
252	Aseguramiento de la disponibilidad	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
253	Aseguramiento de la disponibilidad	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
254	Aseguramiento de la disponibilidad	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
255	Se aplican perfiles de seguridad	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media

N	Control para Frecuencia	Control para Impacto	Medición - Riesgo Residual						
			Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
256	Operación	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
257	Segregación de las redes en dominios	Se aplican perfiles de seguridad	Muy Frecuente	Mayor	1,5	0,77	1,155	48	Alta
258	Sistema de protección perimetral	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
259	Aseguramiento de la disponibilidad	Puesta en producción	Muy Frecuente	Severo	1,5	0,8	1,2	50	Alta
260	Diseño	Se aplican perfiles de seguridad	Improbable	Menor	1	0,5	0,5	21	Media
261	Control de los accesos físicos	Copias de seguridad (backup)	Muy Frecuente	Severo	1,5	0,8	1,2	50	Alta
262	Diseño	Puesta en producción	Improbable	Menor	1	0,5	0,5	21	Media
263	Defensa en profundidad	Se aplican perfiles de seguridad	Muy Frecuente	Severo	1,5	0,8	1,2	50	Alta
264	Control de los accesos físicos	Aseguramiento de la disponibilidad	Improbable	Menor	1	0,5	0,5	21	Media
265	Aseguramiento de la disponibilidad	Aceptación y puesta en operación	Probable	Mayor	1,35	0,77	1,0395	43	Alta
266	Plan de Recuperación de Desastres (DRP)	Copias de seguridad (backup)	Improbable	Menor	1	0,5	0,5	21	Media
267	Formación y concienciación	Aseguramiento de la disponibilidad	Improbable	Menor	1	0,5	0,5	21	Media
268	Aseguramiento de la disponibilidad	Aseguramiento de la disponibilidad	Improbable	Menor	1	0,5	0,5	21	Media
269	Formación y concienciación	Aseguramiento de la disponibilidad	Improbable	Menor	1	0,5	0,5	21	Media
270	Aseguramiento de la disponibilidad	Aseguramiento de la disponibilidad	Improbable	Menor	1	0,5	0,5	21	Media
271	Formación y concienciación	Aseguramiento de la disponibilidad	Improbable	Menor	1	0,5	0,5	21	Media
272	Aseguramiento de la disponibilidad	Aseguramiento de la disponibilidad	Improbable	Menor	1	0,5	0,5	21	Media
273	Aseguramiento de la disponibilidad	Aseguramiento de la disponibilidad	Improbable	Menor	1	0,5	0,5	21	Media
274	Aseguramiento de la disponibilidad	Aseguramiento de la disponibilidad	Improbable	Menor	1	0,5	0,5	21	Media
275	Aseguramiento de la disponibilidad	Aseguramiento de la disponibilidad	Improbable	Menor	1	0,5	0,5	21	Media
276	Aseguramiento de la disponibilidad	Aseguramiento de la disponibilidad	Improbable	Menor	1	0,5	0,5	21	Media

N	Control para Frecuencia	Control para Impacto	Medición - Riesgo Residual						
			Frecuencia	Impacto	Frecuencia	Impacto	RI	RB	Vulnerabilidad
277	Formación y concienciación	Formación y concienciación	Improbable	Menor	1	0,5	0,5	21	Media
278	Formación y concienciación	Formación y concienciación	Improbable	Menor	1	0,5	0,5	21	Media
279	Formación y concienciación	Formación y concienciación	Improbable	Menor	1	0,5	0,5	21	Media
280	Restructuración organizacional	Formación y concienciación	Probable	Mayor	1,35	0,77	1,0395	43	Alta
281	Formación y concienciación	Formación y concienciación	Improbable	Menor	1	0,5	0,5	21	Media
282	Formación y concienciación	Formación y concienciación	Improbable	Menor	1	0,5	0,5	21	Media
283	Restructuración organizacional	Formación y concienciación	Probable	Mayor	1,35	0,77	1,0395	43	Alta
284	Formación y concienciación	Formación y concienciación	Improbable	Menor	1	0,5	0,5	21	Media
285	Formación y concienciación	Formación y concienciación	Improbable	Menor	1	0,5	0,5	21	Media

Se considera entonces que aunque el riesgo residual es considerable, las medidas que se han adoptado están en la capacidad de contrarrestar el nivel de impacto de ambos tipos de vulnerabilidades.

10.2. RECOMENDACIONES DE CONTROL

Sin perjuicio de lo anterior, las falencias en el grupo de “Personal” pueden verse reflejadas en el momento en el que el Plan de Continuidad del negocio, que se establece en el actual Sistema de Gestión de Seguridad Informática, deba ponerse en marcha, esto debido a que es determinante para el engranaje de todas las partes, de la capacidad de comunicación y de integridad que tanto a nivel de tratamiento de amenazas como de puesta en marcha de la contingencia se presenten.

Otros aspecto detectado en el análisis de riesgos, determina que es necesario confirmar si las salvaguardas establecidas son lo suficientemente fuertes para evitar que los riesgos pasen a un nivel de atención inminente, por su lado la comunicación con el Datacenter requiere que cuanto ante se analice la situación y se tomen medidas que den mayor confiabilidad a la prestación del servicio y en la parte de personal se debe analizar y gestionar la salvaguarda correspondiente.

No obstante, es la alta dirección en cabeza de la presidencia ejecutiva de Confecámaras, quien determina de acuerdo con la estrategia del negocio, la evaluación del riesgo, la implementación de los controles de seguridad, y el estudio de la relación costo-beneficio, si un riesgo es mitigado, transferido o aceptado.

Se estima entonces que la Confederación esta en mora de implementar el mayor número de controles posibles y aportar una mejora significativa a los ya existentes, poniendo en conocimiento dichos controles a sus empleados, en concordancia con las políticas declaradas y aceptadas en el sistema de seguridad de la información, puesto que las medidas de seguridad deben alinearse hacia los riesgos más importantes del negocio, garantizando así un óptimo funcionamiento.

11. EVALUACIÓN DE CUMPLIMIENTO BASADO EN ISO 27001:2013 ANEXO A

La Confederación en cabeza de los directores de las áreas de desarrollo y servicios camerales y una vez que se asumió el reto de someter la estructura de seguridad y el análisis de los procesos que abarcan toda a organización, propició varias reuniones iniciales donde se permitió, entre otras cosas, dar la conformación al comité de análisis de riesgos, descrito dentro del actual Plan de Continuidad del Negocio e iniciar el plan de evaluación de la situación real.

Para tal fin y en miras de dar cumplimiento a todos los aspectos posibles que comprender la norma ISO 27001 en su versión 2013, se desarrolló de manera íntegra todo el Anexo A de la norma que entre otras cosas permite:

- Determinar para cada uno de los dominios la aplicabilidad del mismo en la entidad.
- Aplicar el porcentaje de cumplimiento. Esto es de gran importancia no solo para iniciar un proyecto de SGSI sino también para evaluar el funcionamiento posterior del mismo de manera objetiva.
- Dejar un registro de las actividades en cada uno de los dominios en términos que fácilmente puedan ser entendidos.
- Dar una “imagen” general de los procesos que avalúa la norma y como los mismos interactúan de manera contante con todos los demás aspectos de la norma.

El formato que se desarrolló de manera general y en concordancia con los dueños de los procesos, contiene los siguientes campos:

- Nombre ISO 27001: Comprende cada uno de los dominios de la nueva versión de la ISO.

- Control: Descripción del aspecto propio de la norma sujeto a la aplicación y al porcentaje de cumplimiento.

- Aplica: Indica si la implementación del control tiene sentido para la organización.

- % de Cumplimiento: En caso que aplique, este % Indica el grado de implementación del control (0% – 100%) o de la madurez en algún sentido del mismo.

- Situación actual: Evidencia de la implementación total o parcial del control.

- Observaciones: Cualquier dato adicional que valga la pena analizar por parte del encuestador o líder el SGSI.

El formato usado se encuentra en el Anexo 2 de este documento.

El autodiagnóstico se realizó de manera consolidada para finales del 2014 a manera de estado inicial y el mismo autodiagnóstico se efectúo en el presente año para principios de Abril y finales de Junio.

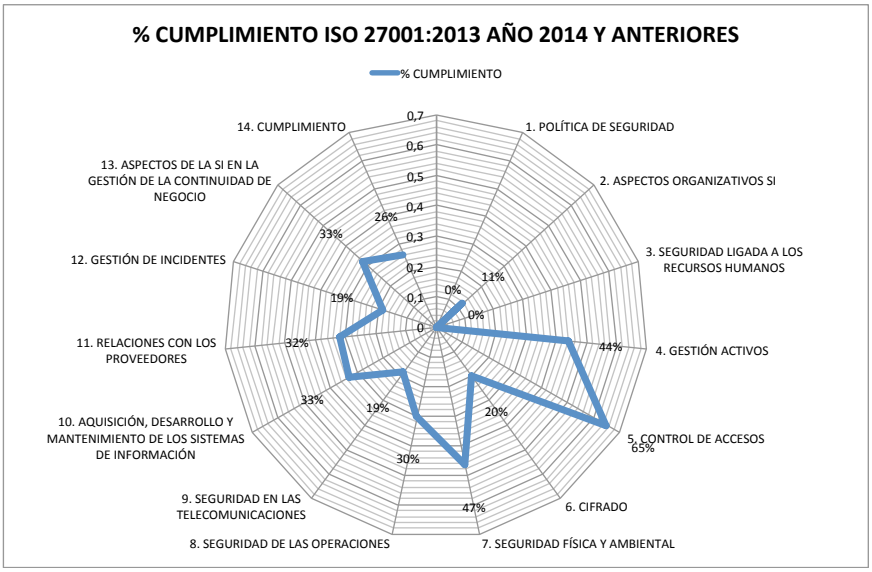
A continuación se presentan los resultados de los tres análisis:

- Análisis 2014

El primer análisis, del cual se evidencian los resultados en la gráfica 3, corresponde a la evaluación inicial que estableció la realidad de la situación en la confederación y la necesidad perentoria de ejecutar un plan de mejoramiento a corto plazo. Esto ligado a la premura con la cual se iniciaron los proyectos de índole nacional relacionados con la Registraduría Nacional y la Superintendencia de Industria y Comercio:

Gráfica 3: Autodiagnóstico según Anexo A, año 2014:

AUTODIAGNOSTICO ANEXO A - ISO 27001:2013 - AÑO 2014 Y ANTERIORES	
NUMERAL ISO 27001	**% CUMPLIMIENTO**
1. POLÍTICA DE SEGURIDAD	0%
2. ASPECTOS ORGANIZATIVOS SI	11%
3. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	0%
4. GESTIÓN ACTIVOS	44%
5. CONTROL DE ACCESOS	65%
6. CIFRADO	20%
7. SEGURIDAD FÍSICA Y AMBIENTAL	47%
8. SEGURIDAD DE LAS OPERACIONES	30%
9. SEGURIDAD EN LAS TELECOMUNICACIONES	19%
10. AQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	33%
11. RELACIONES CON LOS PROVEEDORES	32%
12. GESTIÓN DE INCIDENTES	19%
13. ASPECTOS DE LA SI EN LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO	33%
14. CUMPLIMIENTO	26%



Fuente: El autor

- Análisis 2015 I:

Para el siguiente análisis, el primer trimestre del año 2015, se contó de igual forma con el apoyo de las áreas más representativas en cuanto a cuestiones de tecnología de la confederación, momento en el cual ya se estaban adelantando tareas del SGSI en su etapa de “Planeación“ y de manera temprana la de “Acción”, etapas del siclo PHVA. El autodiagnóstico fue programado como necesidad latente ante encuentros con la Registraduría Nacional, donde solicitaba madurez en los aspectos de seguridad de la entidad y por tal motivo se adelantó el autodiagnóstico para establecer y evaluar si las mejoras se estaban viendo reflejadas en el modelo del SGSI.

Como era de esperarse, algunos dominios aún se encontraban estancados, como el de Control de accesos y Seguridad física y ambiental.

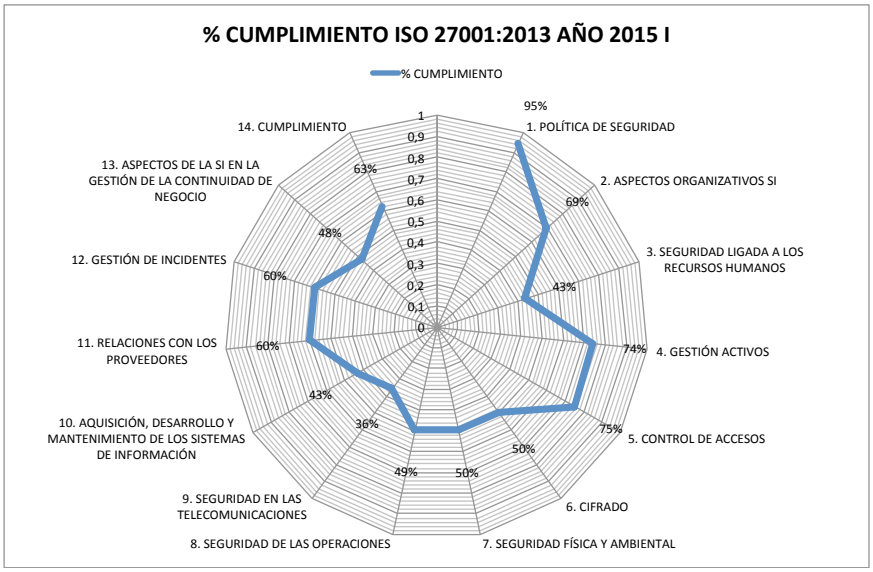
No obstante, otros dominios ya estaban mostrando avances significativos que dejan evidencia de que el modelo aplicado estaba rindiendo resultados palpables.

Por un lado se encuentra un cambio considerable en tema de Políticas de seguridad, donde se pasó de 0% a 95%, demostrando que la implementación había dado un giro radical a la seguridad basada en el estándar aplicado y por otro lado, temas como relaciones con los proveedores y gestión de incidentes habían crecido, principalmente por corresponder a dos de las áreas más involucradas en todos los temas de la recolección de información del SGSI para Confecámaras:

La gráfica 4, Demuestra como las aristas del diagrama crecieron en la mayoría de los aspectos con respecto al año inmediatamente anterior:

Gráfica 4: Autodiagnóstico según Anexo A, año 2015 I

AUTODIAGNOSTICO ANEXO A - ISO 27001:2013 - AÑO 2015 I	
NUMERAL ISO 27001	**% CUMPLIMIENTO**
1. POLÍTICA DE SEGURIDAD	95%
2. ASPECTOS ORGANIZATIVOS SI	69%
3. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	43%
4. GESTIÓN ACTIVOS	74%
5. CONTROL DE ACCESOS	75%
6. CIFRADO	50%
7. SEGURIDAD FÍSICA Y AMBIENTAL	50%
8. SEGURIDAD DE LAS OPERACIONES	49%
9. SEGURIDAD EN LAS TELECOMUNICACIONES	36%
10. AQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	43%
11. RELACIONES CON LOS PROVEEDORES	60%
12. GESTIÓN DE INCIDENTES	60%
13. ASPECTOS DE LA SI EN LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO	48%
14. CUMPLIMIENTO	63%



Fuente: El autor

- Análisis 2015 II:

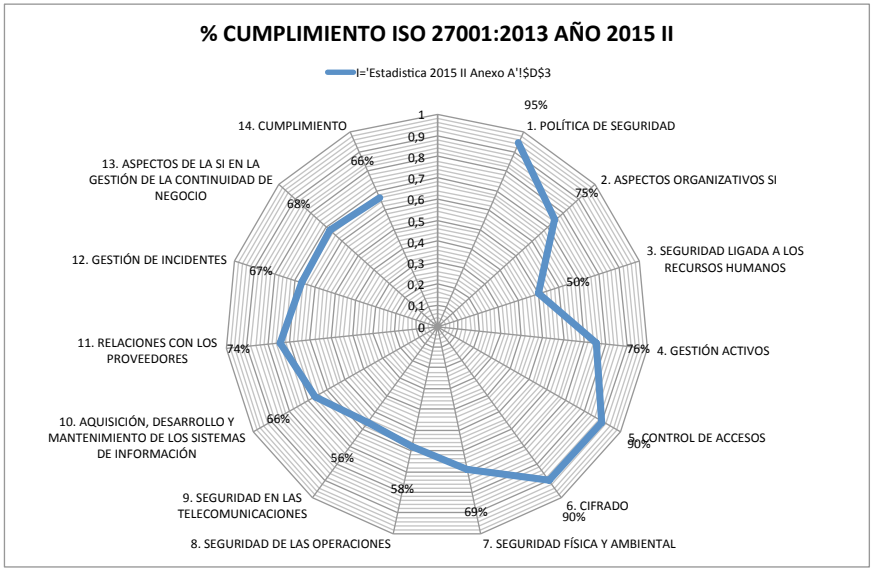
El segundo análisis gestionado para el SGSI de Confecámaras, confirmo lo que se había demostrado en el primer análisis del año 2015, y era que el plan de mejoramiento continuo era ya una realidad y la visión de seguridad y confiabilidad en los procesos de la Confederación estaban dando márgenes muy positivos entre los análisis.

Los resultados más destacados se vieron en temas que se convirtieron en objetivos inmediatos en periodos de exigencia muy cortos; como el del dominio de cifrado, el cual por proyectos de certificados electrónicos tuvo que ser mejorado drásticamente y por ende se pasa en el año 2014 de 20% de aplicación a 90%, lo cual se explica en retos asumidos por la presidencia de la entidad y que competen a proyectos de impacto nacional, donde el compromiso con las Cámaras de Comercio y la Superintendencia de Industria y comercio son totales.

La gráfica 5analiza el comportamiento en su último análisis y permite destacar el buen desempeño que en gestión de seguridad se ha logrado cumplir.

Gráfica 5: Autodiagnóstico según Anexo A, año 2015 II

AUTODIAGNOSTICO ANEXO A - ISO 27001:2013 - AÑO 2015 ii	
NUMERAL ISO 27001	**% CUMPLIMIENTO**
1. POLÍTICA DE SEGURIDAD	95%
2. ASPECTOS ORGANIZATIVOS SI	75%
3. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	50%
4. GESTIÓN ACTIVOS	76%
5. CONTROL DE ACCESOS	90%
6. CIFRADO	90%
7. SEGURIDAD FÍSICA Y AMBIENTAL	69%
8. SEGURIDAD DE LAS OPERACIONES	58%
9. SEGURIDAD EN LAS TELECOMUNICACIONES	56%
10. AQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	66%
11. RELACIONES CON LOS PROVEEDORES	74%
12. GESTIÓN DE INCIDENTES	67%
13. ASPECTOS DE LA SI EN LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO	68%
14. CUMPLIMIENTO	66%



Fuente: El autor

- Análisis 2015 III:

El último análisis programado para el presente año, se ejecutará durante la misma instancia de la primera auditoria interna, la cual se llevará a cabo para finales del mes de Octubre.

En dicho análisis se obtendrá el último estado de la Confederación en temáticas de cumplimiento con el SGSI y el mismo tendrá la particularidad de ser herramienta del área de infraestructura para la planeación estratégica del año 2016 en relación de procesos y presupuesto.

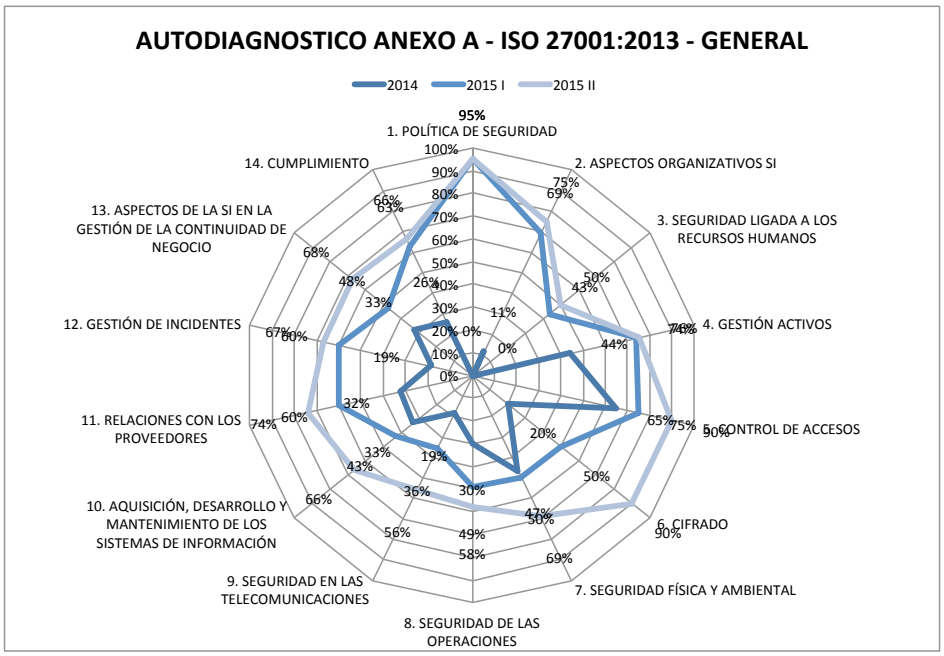
Se espera que el resultado sea el más acercado a un sistema robusto y seguro, ya que actualmente la fase de “hacer” se encuentra en una fase muy importante de

ejecución y por consiguiente encarar la fase de verificación retroalimentará el, hasta ahora joven; SGSI.

Como apartado de conclusión a las evaluaciones ejecutadas durante el transcurso del SGSI, se tiene, de acuerdo a la gráfica 6, la perspectiva de los tres análisis efectuados y la comparación evidente de los mismos:

Gráfica 6: Autodiagnóstico comparativo 2014 – 2015

AUTODIAGNOSTICO ANEXO A - ISO 27001:2013 - GENERAL			
NUMERAL ISO 27001	**2014**	**2015 I**	**2015 II**
1. POLÍTICA DE SEGURIDAD	0%	95%	95%
2. ASPECTOS ORGANIZATIVOS SI	11%	69%	75%
3. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	0%	43%	50%
4. GESTIÓN ACTIVOS	44%	74%	76%
5. CONTROL DE ACCESOS	65%	75%	90%
6. CIFRADO	20%	50%	90%
7. SEGURIDAD FÍSICA Y AMBIENTAL	47%	50%	69%
8. SEGURIDAD DE LAS OPERACIONES	30%	49%	58%
9. SEGURIDAD EN LAS TELECOMUNICACIONES	19%	36%	56%
10. AQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	33%	43%	66%
11. RELACIONES CON LOS PROVEEDORES	32%	60%	74%
12. GESTIÓN DE INCIDENTES	19%	60%	67%
13. ASPECTOS DE LA SI EN LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO	33%	48%	68%
14. CUMPLIMIENTO	26%	63%	66%



Fuente: El autor

12. DECLARACIÓN DE APLICABILIDAD

ANEXO A DE LA NTC-ISO/IEC 27001:2013 (Normativo)
OBJETIVOS DE CONTROL Y CONTROLES
EN “CONFECÁMARAS”

A continuación se presenta una evaluación detallada de la operación tecnológica en la Confederación Colombiana de Cámaras de Comercio, en la cual para cada uno de los 14 dominios se establecen dos situaciones:

- Control: Nivel que destaca la particularidad del dominio y aproxima el estándar ISO a la realidad de la organización.

- Aplicación: Determina cual dimensión del SGSI, herramienta o proceso es las más adecuada para que el control pueda ser ejecutado de manera concreta.

12.1 POLÍTICA DE SEGURIDAD
12.1.1 DIRECTRICES DE LA DIRECCIÓN EN SEGURIDAD INFORMÁTICA

Políticas para la Seguridad Informática

Control: Se debería definir un conjunto de políticas para la Seguridad Informática, aprobado por la dirección, publicado y comunicado a los empleados así como a todas las partes externas relevantes.

Aplicación: La política de Seguridad Informática tiene por objeto proteger los activos de información de la organización, ante cualquier amenaza interna o externa que pueda afectar integridad, disponibilidad, confiabilidad, autenticidad y trazabilidad.

La política de Seguridad Informática aplica sobre todo el personal de la Organización.

La política tiene por objetivos:

Realizar la gestión del riesgo necesaria para identificar posibles riesgos y amenazas, de modo que se puedan adoptar las medidas necesarias para su debida atención, utilizando las metodologías necesarias para la gestión de los riesgos.

- Proteger la información del acceso no autorizado por parte de personal interno o externo.
- Garantizar la confidencialidad de la información.
- Garantizar la integridad de la información evitando su pérdida o deterioro.
- Garantizar la disponibilidad de la información, siempre y cuando así sea requerido.
- Garantizar la autenticidad de la información.
- Garantizar la trazabilidad de la información.
- Cumplir con la normatividad vigente en no sólo en materia de Seguridad Informática sino también en cuanto a las normatividad que rige a los subprocesos de los Departamentos de la empresa.
- Crear una cultura de Seguridad Informática en todo el personal del Departamento frente a la Seguridad Informática y frente a la responsabilidad de proteger y preservar los activos de información que allí se manejan.

- Revisión de las políticas para la Seguridad Informática

Control: Las políticas para la Seguridad Informática se deberían planificar y revisar con regularidad o si ocurren cambios significativos para garantizar su idoneidad, adecuación y efectividad.

Aplicación: Trimestralmente se debe realizar la evaluación de la Política de seguridad y los componentes que esta desprenda dentro de la Organización, con el fin de establecer directrices para revisar todo el Sistema de Gestión de Seguridad Informática, de tal forma que se asegure conveniencia, eficacia frente a las necesidades de los clientes y el cumplimiento de todos los objetivos propuestos.

Igualmente se deben revisar las acciones preventivas y correctivas que durante este periodo se hayan implementado con el fin de establecer la coherencia con el compromiso de mejora continua de la Organización y todo el Sistema de Seguridad Informática.

12.2 ASPECTOS ORGANIZATIVOS SI

12.2.1 ORGANIZACIÓN INTERNA

- Asignación de responsabilidades para la SI

Control: Se deberían definir y asignar claramente todas las responsabilidades para la Seguridad Informática.

Aplicación: El comité de Seguridad Informática está constituido por los responsables de las Unidades afectables por el proyecto de Análisis y Gestión de Riesgos, así como por los responsables de sistemas y de la gestión dentro de dichas Unidades.

Dicho comité tendrá unos roles comunes:

- Revisar y proponer cambios de la política de seguridad a la dirección de la Organización, igualmente informará todo lo relacionado en materia de seguridad.
- Monitorear los cambios que surjan de los riesgos que afectan los recursos informáticos.
- Analizar y aprobar iniciativas que apalanquen la política y los objetivos de la Seguridad Informática.
- Evaluar y coordinar la planificación e implementación de controles.
- Difundir la política, los objetivos, controles y todo lo relacionado con la Seguridad Informática.
- Promover la mejora continua y la aplicación de todas las actividades que se establecen para mantener la Seguridad Informática de la Organización.

Dentro de este comité se deberá definir las responsabilidades y los roles que cumplirán:

Coordinador: Coordinara todas las acciones del comité de seguridad e impulsara la implementación de la Política y los objetivos de la Seguridad Informática.

Responsable de Sistemas: Cumplirá las acciones relacionadas con la seguridad de todos los sistemas de información que tiene la Organización y los que se proyectan que entrarán en funcionamiento, de tal forma que se encuentren alineados con la política y objetivos de la Seguridad Informática definidos en la Organización.

También desarrollará con su equipo de trabajo, los requerimientos de Seguridad Informática establecidos para la administración, operación y mantenimiento de todos los recursos informáticos de acuerdo a lo establecido en los lineamientos para el cumplimiento de la Seguridad Informática.

Responsable de Gestión Humana: Comunicará a toda la Organización las responsabilidades que tiene cada funcionario para cumplir las normas, procedimientos, política y objetivos de Seguridad Informática.

Igualmente será el encargado de notificar los cambios que surjan en todos los documentos relacionados con la Seguridad Informática, velará por las firmas de los acuerdos de confidencialidad y todas las capacitaciones que hubiese lugar en materia de seguridad.

Responsable Legal: Verificará el cumplimiento de todos los contratos, acuerdos u otra documentación con los empleados y terceros, también prestará asesoría cuando sea necesario en materia de Seguridad Informática.

Propietarios de información: Clasificarán la información de acuerdo al grado de confidencialidad necesario, y dicha clasificación deberá ser documentada y constantemente actualizada, definirán los permisos de acceso de acuerdo a sus roles y responsabilidades dentro de la Organización

- Segregación de tareas

Control: Se deberían segregar tareas y las áreas de responsabilidad ante posibles conflictos de interés con el fin de reducir las oportunidades de una modificación no autorizada o no intencionada, o el de un mal uso de los activos de la organización.

Aplicación: Se separará la gestión o ejecución de ciertas tareas o áreas de responsabilidad, a fin de reducir el riesgo de modificaciones no autorizadas o mal uso de la información o los servicios por falta de independencia en la ejecución de funciones críticas.

Si este método de control no se pudiera cumplir en algún caso, se implementarán controles como:

- Monitoreo de las actividades.
- Registros de auditoría y control periódico de los mismos.
- Supervisión por parte del Área de Auditoría de la Organización o en su defecto quien sea propuesto para tal efecto, siendo independiente al área que genera las actividades auditadas.

Así mismo, se documentará la justificación formal por la cual no fue posible efectuar la segregación de funciones.

Se asegurará la independencia de las funciones de auditoría de seguridad, tomando recaudos para que ninguna persona pueda realizar actividades en áreas de responsabilidad única sin ser monitoreada, y la independencia entre el inicio de un evento y su autorización, considerando los siguientes puntos:

- Separar actividades que requieren acuerdo de complicidad para defraudar, por ejemplo efectuar una orden de compra y verificar que la mercadería fue recibida.
- Diseñar controles, si existe peligro de connivencia de manera tal que dos o más personas estén involucradas, reduciendo la posibilidad de conspiración.

- Contacto con las autoridades

Control: Se deberían mantener los contactos apropiados con las autoridades pertinentes.

Aplicación: La Organización deberá establecer y mantener un contacto permanente con autoridades relevantes (Policía, Fiscalía, Bomberos, Defensa Civil), para que puedan ser contactados de manera oportuna en el caso de que se presente un incidente de seguridad, que comprometa la Seguridad Informática.

- Contacto con grupos de interés especial

Control: Se debería mantener el contacto con grupos o foros de seguridad especializados y asociaciones profesionales.

Aplicación: La Organización deberá establecer y mantener un contacto permanente con entidades, grupos, foros y cualquier tipo de organización, especializados en temas de Seguridad Informática, a fin de obtener información actualizada y, asesoría frente a un incidente de seguridad, que comprometa la Seguridad Informática.

- Seguridad Informática en la gestión de proyectos

Control: Se debería contemplar la Seguridad Informática en la gestión de proyectos e independientemente del tipo de proyecto a desarrollar por la organización, incluidos los convenios que a bien Confecámaras establezca con terceros.

Aplicación: La Organización deberá aplicar todas y cada una de las políticas establecidas en la presente declaración de aplicabilidad, para todo los proyectos que desarrolle, indiferente si se trata de proyectos informáticos o de cualquier otra índole, a fin de garantizar la confidencialidad, integridad, disponibilidad, trazabilidad y la autenticidad de la información que se utilice o se genere como producto del desarrollo de dichos proyectos.

12.2.2 DISPOSITIVOS PARA MOVILIDAD Y TELETRABAJO

- Política de uso de dispositivos para movilidad

Control: Se debería establecer una política formal y se deberían adoptar las medidas de seguridad adecuadas para la protección contra los riesgos derivados del uso de los recursos de informática móvil y las telecomunicaciones.

Aplicación: Cuando se utilizan dispositivos informáticos móviles se debe tener especial cuidado en garantizar que no se comprometa la información de la Organización.

Se deberá tener en cuenta en este sentido, cualquier dispositivo móvil y/o removible que pueda contener información confidencial de la Organización, que sea susceptible de sufrir un incidente que comprometa su seguridad.

Se desarrollarán procedimientos adecuados para estos dispositivos, que abarquen los siguientes conceptos:

- La protección física necesaria
- El acceso seguro a los dispositivos
- La utilización de los dispositivos en lugares públicos.
- El acceso a los sistemas de información y servicios de la Organización a través de dichos dispositivos.
- Las técnicas criptográficas a utilizar para la transmisión de información clasificada.
- Los mecanismos de resguardo de la información contenida en los dispositivos.
- La protección contra software malicioso.

La utilización de dispositivos móviles incrementa la probabilidad de ocurrencia de incidentes del tipo de pérdida, robo o hurto. En consecuencia deberá entrenarse especialmente al personal que los utilice. Se desarrollarán normas y procedimientos sobre los cuidados especiales a observar ante la posesión de dispositivos móviles, que contemplarán las siguientes recomendaciones:

- Permanecer siempre cerca del dispositivo.
- No dejar desatendidos los equipos.
- No llamar la atención acerca de portar un equipo valioso.
- No poner identificaciones de la Organización en el dispositivo, salvo los estrictamente necesarios.
- No poner datos de contacto técnico en el dispositivo.
- Mantener cifrada la información clasificada.

Por otra parte, se crearán procedimientos que permitan al propietario del dispositivo reportar rápidamente cualquier incidente sufrido y mitigar los riesgos a los que eventualmente estuvieran expuestos los sistemas de información de la Organización, los que incluirán:

- Revocación de las credenciales afectadas
- Notificación a grupos de Trabajo donde potencialmente se pudieran haber comprometido recursos.

12.3 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS
12.3.1 ANTES DE LA CONTRATACIÓN

- Investigación de antecedentes

Control: Se deberían realizar revisiones de verificación de antecedentes de los candidatos al empleo en concordancia con las regulaciones, ética y leyes relevantes y deben ser proporcionales a los requerimientos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.

Aplicación: El Departamento de Gestión Humana, o quien sea responsable de los procesos de selección, una vez tenga el análisis de la hoja de vida de los personas aptas al cargo, (cumplimiento de requisitos del perfil), debe verificar la información que los aspirantes han suministrado en cada una de sus hojas de vida, como referencias laborales, familiares, datos personales, entre otros.

Una vez se cumpla con el porcentaje establecido de la primera fase de selección, el proceso podrá continuar a las fases de examen técnico de conocimientos, prueba sicotécnica y entrevista sicológica.

Este proceder deberá ser documentado en el respectivo procedimiento de selección de personal, definiendo los criterios y las limitaciones de las verificaciones, así como la aplicación (procesos, internos, externos directos, externos con terceros (contratistas, agencias de empleo))

- Términos y condiciones de contratación

Control: Como parte de su obligación contractual, empleados, contratistas y terceros deberían aceptar y firmar los términos y condiciones del contrato de empleo, el cual establecerá sus obligaciones y las obligaciones de la organización para la seguridad de información.

Aplicación: Al hacer parte de una empresa, todos los funcionarios deben recibir unas responsabilidades, por tanto, como parte de la obligación contractual se debe estar de acuerdo en firmar los términos y condiciones del contrato laboral, el cual define las responsabilidades y las de la Organización.

Dentro de los términos y condiciones que se definan en material de Seguridad Informática, se debe mencionar:

- Los acuerdos de confidencialidad

- La responsabilidad con preservación material de los activos de información.
- La responsabilidad en el manejo de la información
- Los acuerdos de propiedad intelectual
- El compromiso que adquiere para contribuir a la mejora continua del sistema de Seguridad Informática.

12.3.2 DURANTE LA CONTRATACIÓN

- Responsabilidades de gestión

Control: La Dirección debería requerir a empleados, contratistas y usuarios de terceras partes aplicar la seguridad en concordancia con las políticas y los procedimientos.

Aplicación: La Organización tendrá la obligación de dar a conocer a los empleados, contratistas y usuarios de terceras partes, las políticas definidas por la organización en materia de Seguridad Informática. Así mismo, será estricta en el cumplimiento de las mismas, tomando las medidas disciplinarias o legales del caso, cuando dichas políticas no sean cumplidas por el personal, contratistas y usuarios de terceras partes.

- Concienciación, educación y capacitación en SI

Control: Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.

Aplicación: La Organización debe asegurar que todo su personal conozca las políticas y lineamientos que están definidos para llevar a cabo un sistema de Seguridad Informática.

Que dichas políticas y lineamientos deben darse a conocer en los procesos de inducción y re inducción del personal, mostrando igualmente los impactos, amenazas y preocupaciones que se tienen identificados respecto a la seguridad de información.

Desde el comité de dirección deben crearse iniciativas que permitan generar recordación y conciencia sobre la importancia de aplicar las políticas y lineamientos definidos para la Seguridad Informática. Igualmente estas deben generar motivación y dejar herramientas de reconocimiento de problemas e incidentes de seguridad, que les permita atender y responder de acuerdo a sus roles y los lineamientos definidos por la Organización.

- Proceso disciplinario

Control: Debería existir un proceso formal disciplinario comunicado a empleados que produzcan brechas en la seguridad.

Aplicación: Cuando se presenten incidentes que involucren la Seguridad Informática por parte de los empleados de la Organización, la entidad aplicará lo establecido dentro de su Reglamento Interno de Trabajo, con el fin de tomar las medidas disciplinarias para el caso.

12.3.4 CESE O CAMBIO DE PUESTO DE TRABAJO

- Cese o cambio de puesto de trabajo

Control: Las responsabilidades para ejecutar la finalización de un empleo o el cambio de éste deberían estar claramente definidas, comunicadas a empleado o contratista y asignadas efectivamente.

Aplicación: Cuando haya un cambio de responsabilidades o se finalice la relación contractual entre personas y la Organización, la entidad tendrá un procedimiento que incluya:

- Acuerdo de confidencialidad.
- Condiciones Post-empleo.
- Cambios de responsabilidades.
- Retorno de Activos.
- Retorno de Información.
- Entrega de Documentación.

12.4 GESTIÓN ACTIVOS

12.4.1 RESPONSABILIDAD SOBRE LOS ACTIVOS

- Inventario de activos

Control: Todos los activos deberían estar claramente identificados, confeccionando y manteniendo un inventario con los más importantes.

Aplicación: Confecámaras, por cada una de sus dependencias deberá tener identificados los activos de información que maneja, su valor e importancia.

Igualmente deberán ser identificados los activos de información críticos, entendiéndose éstos como cualquier información, sistema, equipo o servicio que la Organización considera clave para soportar su operación, metas y objetivos.

- Propiedad de los activos

Control: Toda la información y activos del inventario asociados a los recursos para el tratamiento de la información deberían pertenecer a una parte designada de la Organización.

Aplicación: En el control anterior, se identificaron los activos con su respectivo responsable, este deberá asegurar que la información y los activos asociados con su procesamiento estén debidamente clasificados de manera correcta, igualmente deberá establecer los controles necesarios para asignar el acceso a éstos.

El responsable de los activos también deberá mantener actualizada la información del activo, sus estados, sus sistemas asociados y si aún sigue clasificado como activo de información crítico.

- Uso aceptable de los activos

Control: Se deberían identificar, documentar e implantar regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información.

Aplicación: Cada una de las dependencias de La Organización debe clasificar su información sea física o electrónica, de acuerdo a las necesidades que tiene la dependencia para compartir o restringir la información, igualmente para esta clasificación deberá tener en cuenta la evaluación que determina el impacto negativo si por cualquier abuso en su manejo pudiera provocar al negocio en términos financieros, administrativos o legales.

De acuerdo a lo anterior, los funcionarios deberán aceptar las reglas definidas por la Organización para el buen uso de la información.

A cada uno de los funcionarios se le entregará la información de acuerdo a su competencia, sus roles y responsabilidades, e igualmente se le indicará la clasificación que ésta tiene dentro de la Organización (restringida, pública, de uso interno, confidencial)

El acceso a la información que reposa en el Archivo Central sólo podrá darse a modo de consulta, según la competencia y deberá hacerse en presencia del responsable del Archivo central.

Dentro del Archivo se llevará registro de todas las consultas solicitadas, identificando fechas, horas y solicitantes de la información.

El acceso a la información que reposa en los diferentes sistemas de información se dará de acuerdo a sus funciones y nivel de competencia.

El acceso de consulta a esta información será evaluado por los jefes inmediatos y de acuerdo a sus roles y responsabilidades.

- Devolución de activos

Control: Todos los empleados y usuarios de terceras partes deberían devolver todos los activos de la organización que estén en su posesión/responsabilidad una vez finalizado el acuerdo, contrato de prestación de servicios o actividades relacionadas con su contrato de empleo

Aplicación: El Departamento de Gestión Humana para realizar la respectiva liquidación al terminar el contrato laboral deberá exigir un paz y salvo firmado por las oficinas

Gestión documental
Control interno y calidad
Contabilidad
Jefe inmediato

Ellas certificarán que el funcionario se encuentra a paz y salvo y no existen novedades a tener en cuenta a la hora de su liquidación.

12.4.2 CLASIFICACIÓN DE LA INFORMACIÓN

- Directrices de clasificación

Control: La información debería clasificarse en relación a su valor, requisitos legales, sensibilidad y criticidad para la Organización.

Aplicación: Cada una de las dependencias de La Organización debe clasificar su información sea física o electrónica, de acuerdo a las necesidades que tiene la dependencia para compartir o restringir la información, igualmente para esta clasificación deberá tener en cuenta la evaluación que determina el impacto negativo si por cualquier abuso en su manejo pudiera provocar al negocio en términos financieros, administrativos o legales.

Esta clasificación deberá realizarla el responsable de los activos de información y deberá evaluar constantemente su clasificación en caso de que sea necesario replantearla.

Dentro de las directrices de clasificación de la información, La Organización ha definido la información así:

Uso interno: Es la información que soporta el día a día de cada uno de los procesos, la cual puede ser difundida al interior de la Organización, nunca a proveedores o personal externo.

Pública: Es la información que divulga la unidad de comunicación a través de boletines de prensa, página de internet, volantes, publicidad (radio, televisión) y que no representa amenaza ni daño alguno a la Organización a nivel de procesos, sistemas de información e imagen.

Confidencial: La información clasificada como confidencial se describe como crítica y por ello debe ser tratada y protegida con atención. El uso inadecuado de esta puede ocasionar impactos negativos dentro de las operaciones de la Organización. Dentro de esta información tenemos los presupuestos, las actas de Junta directiva, información de base de datos de proveedores, iniciativas de nuevos negocios, contraseñas, direccionamientos IP de la Organización entre otros.

Restringida: Es aquella información cuyo conocimiento debe estar limitado en términos generales. Dicha información si es conocida por personas no autorizadas, o se divulgara de forma general, podría perjudicar el patrimonio o el buen nombre de la Organización o alguno de sus funcionarios.

- Etiquetado y manipulado de la información

Control: Se debería desarrollar e implantar un conjunto apropiado de procedimientos para el etiquetado y tratamiento de la información, de acuerdo con el esquema de clasificación adoptado por la organización.

Aplicación: De acuerdo a las directrices de clasificación de la información, por cada definición, deben elaborarse lineamientos a seguir para realizar el copiado, la impresión, el almacenamiento, la transmisión electrónica, el intercambio físico y su destrucción.

- Los documentos con información del tipo “restringida” deben ser controlados por medio de copias individuales perfectamente numeradas y llevar un registro de las personas que las tienen.

- La copia o transferencia por cualquier medio (electrónico, magnético, en papel) de información “restringida” debe estar autorizada y controlada.
- Todos los documentos del tipo “restringida” y “confidencial” deben conservarse bajo llave.
- El envío de documentos con esta clasificación, debe hacerse por medio de canales seguros información tales como mensajería privada, correo electrónico encriptado, entrega personal. Es importante evitar el uso del servicio postal, fax, internet o medios no controlados para su envío.
- Toda recepción de información sensible debe acusar formalmente de recibido.
- El envío físico de información sensible debe hacerse por medio de paquetes debidamente cerrados y que no permitan observar su contenido.
- De ser necesario, debe considerarse un centro de destrucción de documentos restringidos o confidenciales que garantice la no reutilización de la información. La destrucción de registros e información de la empresa debe ser formalmente autorizada por la alta dirección de la Unidad Administrativa a la que pertenece.
- La información sensible debe reflejar por medio de una leyenda apropiada, la clasificación a la que pertenece, sin importar la forma o medio en la que se encuentre.
- La información de la Organización que se utilice para ofrecer conferencias, discursos o presentaciones abiertas debe llevar la autorización del dueño de la información y en su caso, de la Unidad Administrativa.

- Manipulación de activos

Control: Se deberían desarrollar e implantar procedimientos para la manipulación de los activos acordes con el esquema de clasificación de la información adoptado por la organización.

Aplicación: El adecuado manejo de todos los activos en cada una de las dependencias de la Organización corresponderá al respectivo usuario. El jefe de área o departamento responderá por perdidas, daños o deterioro por mal uso.

En todo caso, el acceso a dichos activos dependerá directamente de las funciones del usuario, lo cual será definido por el Jefe de Gestión Humana y el Jefe del Área a la que pertenezca el usuario, quedando dicha responsabilidad por escrito y aceptada, de la misma manera, por el usuario.

12.4.3 MANEJO DE LOS SOPORTES DE ALMACENAMIENTO

- Gestión de soportes extraíbles

Control: Se deberían establecer procedimientos para la gestión de los medios informáticos removibles acordes con el esquema de clasificación adoptado por la organización.

Aplicación: El Departamento de Sistemas implementará procedimientos para la administración de medios informáticos removibles, como cintas, discos, casetes e informes impresos. El cumplimiento de los procedimientos se hará de acuerdo al objetivo 9. CONTROL DE ACCESOS.

Se deberán considerar las siguientes acciones para la implementación de los procedimientos:

- Eliminar de forma segura los contenidos, si ya no son requeridos, de cualquier medio reutilizable que ha de ser retirado o reutilizado por la Organización (ver objetivo 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento)
- Requerir autorización para retirar cualquier medio de la Organización y realizar un control de todos los retiros a fin de mantener un registro de auditoría.
- Almacenar todos los medios en un ambiente seguro y protegido, de acuerdo con las especificaciones de los fabricantes o proveedores.

Se documentarán todos los procedimientos y niveles de autorización, en concordancia con el objetivo 8. GESTIÓN ACTIVOS.

- Eliminación de soportes

Control: Se deberían eliminar los medios de forma segura y sin riesgo cuando ya no sean requeridos, utilizando procedimientos formales.

Aplicación: El Departamento de Sistemas definirá procedimientos para la eliminación segura de los medios de información respetando la normatividad vigente.

Los procedimientos deberán considerar que los siguientes elementos requerirán almacenamiento y eliminación segura:

- Documentos en papel.
- Voces u otras grabaciones.
- Papel carbón.
- Informes de salida.
- Cintas de impresora de un solo uso.
- Cintas magnéticas.
- Discos o casetes removibles.

- Medios de almacenamiento óptico (todos los formatos incluyendo todos los medios de distribución de software del fabricante o proveedor).
- Listados de programas.
- Datos de prueba.
- Documentación del sistema.

Así mismo, se debe considerar que podría ser más eficiente disponer que todos los medios sean recolectados y eliminados de manera segura, antes que intentar separar los ítems sensibles.

- Soportes físicos en tránsito

Control: Se deberían proteger los medios que contienen información contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los límites físicos de la organización.

Aplicación: Los procedimientos de transporte de medios informáticos entre diferentes puntos (envíos postales y mensajería) deberán contemplar:

- La utilización de medios de transporte o servicios de mensajería confiables. El propietario de la información a transportar determinará qué servicio de mensajería se utilizará conforme la criticidad de la información a transmitir.
- Suficiente embalaje para envío de medios a través de servicios postales o de mensajería, siguiendo las especificaciones de los fabricantes o proveedores.
- La adopción de controles especiales, cuando resulte necesario, a fin de proteger la información sensible contra divulgación o modificación no autorizadas. Entre los ejemplos se incluyen:
- Uso de recipientes cerrados.
- Entrega en mano.
- Embalaje a prueba de apertura no autorizada (que revele cualquier intento de acceso).
- En casos excepcionales, división de la mercadería a enviar en más de una entrega y envío por diferentes rutas.

12.5 CONTROL DE ACCESO

12.5.1 REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESOS

- Política de control de accesos

Control: Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización.

Aplicación: Para la aplicación de controles de acceso, la Organización contemplará los siguientes aspectos:

- Identificar los requerimientos de seguridad de cada una de las aplicaciones.
- Identificar toda la información relacionada con las aplicaciones.
- Establecer criterios coherentes entre ésta política y la política de clasificación de la información (Ver objetivo CLASIFICACIÓN DE LA INFORMACIÓN).
- Identificar la legislación aplicable y las obligaciones contractuales con respecto a la protección del acceso a datos y servicios.
- Definir los perfiles de acceso de usuarios estándar, comunes a cada categoría de puestos de trabajo.
- Administrar los derechos de acceso en un ambiente distribuido y de red, que reconozcan todos los tipos de conexiones disponibles.

- Control de acceso a las redes y servicios asociados

Control: Se debería proveer a los usuarios de los accesos a redes y los servicios de red para los que han sido expresamente autorizados a utilizar.

Aplicación: Las conexiones no seguras a los servicios de red pueden afectar a toda la Organización, por lo tanto, se controlará el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios, no comprometan la seguridad de los mismos.

El Departamento de Sistemas tendrá a cargo el otorgamiento del acceso a los servicios y recursos de red, únicamente de acuerdo a la solicitud formal del titular del área que lo solicite.

Este control es particularmente importante para las conexiones de red a aplicaciones que procesen información clasificada o aplicaciones críticas, o a usuarios que utilicen el acceso desde sitios de alto riesgo, por ejemplo áreas públicas o externas que están fuera de la administración y del control de seguridad de la Organización.

Para ello, se desarrollarán procedimientos para la activación y desactivación de derechos de acceso a las redes, los cuales comprenderán:

- Identificar las redes y servicios de red a los cuales se permite el acceso.
- Realizar normas y procedimientos de autorización para determinar las personas y las redes y servicios de red a los cuales se les otorgará el acceso.
- Establecer controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red.

12.5GESTIÓN DE ACCESO DE USUARIO

- Gestión de altas/bajas en el registro de usuarios

Control: Debería existir un procedimiento formal de alta y baja de usuarios con objeto de habilitar la asignación de derechos de acceso.

Aplicación: El Departamento de Sistemas de la Organización, definirá un procedimiento para el registro de usuarios, así como para otorgar y revocar acceso a los sistemas y la información de la Organización; dicho procedimiento deberá contemplar lo siguiente:

- Utilizar identificadores de usuario únicos, de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo empleado. El uso de identificadores grupales sólo debe ser permitido cuando sean convenientes para el trabajo a desarrollar debido a razones operativas.
- Verificar que el usuario tiene la respectiva autorización para el uso del sistema, base de datos o servicio de información.
- Verificar que el nivel de acceso otorgado es adecuado para el propósito de la función del usuario y es coherente con la Política de Seguridad de la Organización, por ejemplo que no comprometa la separación de tareas.
- Entregar a los usuarios por escrito sus derechos de acceso.
- Requerir que los usuarios firmen declaraciones señalando que comprenden y aceptan las condiciones para el acceso.
- Garantizar que los proveedores de servicios no otorguen acceso hasta que se hayan completado los procedimientos de autorización.
- Mantener un registro formal de todas las personas registradas para utilizar el servicio.
- Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización, se desvincularon de la Organización o sufrieron la pérdida/robo de sus credenciales de acceso.
- Efectuar revisiones periódicas con el objeto de:
- Cancelar identificadores y cuentas de usuario redundantes
- Inhabilitar cuentas inactivas por más de 30 días.
- Eliminar cuentas inactivas por más de 60 días.

En el caso de existir excepciones, deberán ser debidamente justificadas y aprobadas.

- Garantizar que los identificadores de usuario redundantes no se asignen a otros usuarios.

- Incluir cláusulas en los contratos de personal y de servicios que especifiquen sanciones si el personal o las personas externas que prestan un servicio intentan accesos no autorizados.

- Gestión de los derechos de acceso asignados a usuarios

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

Aplicación: tanto para la asignación como para la revocación de derechos de acceso de todos los tipos de usuarios y para todos los tipos de sistemas y servicios de la Organización, ésta tendrá un protocolo mediante el cual el Jefe de Gestión Humana y el Jefe de Área a la que pertenece el usuario, establecerán o revocarán dichos derechos de acceso, lo cual debe ser notificado al Área de Sistemas para proceder con la asignación o revocación de dichos derechos de acceso.

- Gestión de los derechos de acceso con privilegios especiales

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

Aplicación: Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente.

Los sistemas multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal. Se deben tener en cuenta los siguientes pasos:

- Identificar los privilegios asociados a cada producto del sistema, por ejemplo sistema operativo, sistema de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los productos.
- Asignar los privilegios a individuos sobre la base de la necesidad de uso y evento por evento, por ejemplo el requerimiento mínimo para su rol funcional.
- Mantener un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no deben ser otorgados hasta que se haya completado el proceso formal de autorización.
- Establecer un período de vigencia para el mantenimiento de los privilegios (en base a la utilización que se le dará a los mismos) luego del cual los mismos serán revocados.

- Promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.

Los jefes de cada área serán los encargados de aprobar la asignación de privilegios a usuarios y solicitar su implementación, lo cual será supervisado por el Departamento de Sistemas.

Gestión de información confidencial de autenticación de usuarios

Control: La asignación de información confidencial para la autenticación debería ser controlada mediante un proceso de gestión controlado.

Aplicación: La asignación de contraseñas se controlará a través de un proceso de administración formal, mediante el cual deben respetarse los siguientes pasos:

- Requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto y las contraseñas de los grupos de trabajo exclusivamente entre los miembros del grupo. Esta declaración bien puede estar incluida en el Acuerdo de Confidencialidad (ver objetivo 13.2.4 Acuerdos de confidencialidad y secreto).
- Garantizar que los usuarios cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan al sistema. Las contraseñas provisorias, que se asignan cuando los usuarios olvidan su contraseña, sólo debe suministrarse una vez identificado el usuario.
- Generar contraseñas provisorias seguras para otorgar a los usuarios. Se debe evitar la participación de terceros o el uso de mensajes de correo electrónico sin protección (texto claro) en el mecanismo de entrega de la contraseña y los usuarios deben dar acuse de recibo cuando la reciban.
- Almacenar las contraseñas sólo en sistemas informáticos protegidos.
- Configurar los sistemas de tal manera que:
- Las contraseñas tengan 10 caracteres de longitud.
- Suspendan o bloqueen permanentemente al usuario luego de 3 intentos de entrar con una contraseña incorrecta (deberá pedir la rehabilitación ante quien corresponda),
- Solicitar el cambio de la contraseña cada 30 días.

- Revisión de los derechos de acceso de los usuarios

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

Aplicación: A fin de mantener un control eficaz del acceso a los datos y servicios de información, el jefe de área correspondiente en conjunto con el Departamento

de Sistemas llevará a cabo un proceso de manera semestral, con el fin de revisar los derechos de acceso de los usuarios de su área, contemplando lo siguiente:

- Revisar los derechos de acceso de los usuarios a intervalos de 6 meses.
- Revisar las autorizaciones de privilegios especiales de derechos de acceso a intervalos de 3 meses
- Revisar las asignaciones de privilegios a intervalos de 6 meses, a fin de garantizar que no se obtengan privilegios no autorizados.

- Retirada o adaptación de los derechos de acceso

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

Aplicación: El Departamento de Gestión Humana deberá notificar al funcionario con un término de 10 días hábiles la terminación o cambio de contrato laboral indicando que deberá dejar saneado su inventario así como entregar todos los pendientes de su cargo a la fecha a la persona que la misma Organización designe.

Esta notificación deberá ir con copia al Departamento de Sistemas, con el fin de que los roles que tenga en los diferentes aplicaciones sean deshabilitados.

12.5.1 RESPONSABILIDADES DEL USUARIO

- Uso de información confidencial para la autenticación

Control: Se debería exigir a los usuarios el uso de las buenas prácticas de seguridad de la organización en el uso de información confidencial para la autenticación.

Aplicación: Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas.

Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.

Los usuarios deben cumplir las siguientes directivas:

- Mantener las contraseñas en secreto.

- Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
- Seleccionar contraseñas de calidad, las cuales:
- Sean fáciles de recordar.
- No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo nombres, números de teléfono, fecha de nacimiento, etc.
- No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos, en lo posible que incluyan también símbolos.
- Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.
- Cambiar las contraseñas provisorias en el primer inicio de sesión (“log on”).
- Notificar de acuerdo a lo establecido en el objetivo 16.1 GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA Y MEJORAS, cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

Si los usuarios necesitan acceder a múltiples servicios o plataformas y se requiere que mantengan múltiples contraseñas, se notificará a los mismos que pueden utilizar una única contraseña para todos los servicios que brinden un nivel adecuado de protección de las contraseñas almacenadas y en tránsito.

12.5.2 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES

- Restricción del acceso a la información

Control: Se debería restringir el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida.

Aplicación: Los usuarios de sistemas de aplicación, con inclusión del personal de soporte, tendrán acceso a la información y a las funciones de los sistemas de aplicación de conformidad con la Política de control de acceso definida, sobre la base de los requerimientos de cada aplicación, y conforme a la Política de la Organización para el acceso a la información, (ver objetivo 9.1.1 Política de control de accesos).

Se aplicarán los siguientes controles, para brindar apoyo a los requerimientos de limitación de accesos:

- Proveer una interfaz para controlar el acceso a las funciones de los sistemas de aplicación. El jefe del área correspondiente será responsable de la adjudicación de accesos a las funciones. En el caso de que las actividades involucradas en el otorgamiento de acceso revistan un carácter

técnico elevado, las mismas serán llevadas a cabo por personal del Departamento de Sistemas, conforme a una autorización formal emitida por el jefe de área.

- Restringir el conocimiento de los usuarios acerca de la información o de las funciones de los sistemas de aplicación a las cuales no sean autorizados a acceder, con la adecuada edición de la documentación de usuario.
- Controlar los derechos de acceso de los usuarios, por ejemplo, lectura, escritura, supresión y ejecución.
- Garantizar que las salidas de los sistemas de aplicación que administran información sensible, contengan sólo la información que resulte pertinente para el uso de la salida, y que la misma se envíe solamente los equipos y ubicaciones autorizadas.
- Revisar periódicamente dichas salidas a fin de garantizar la remoción de la información redundante.
- Restringir el acceso a la información por fuera del sistema encargado de su procesamiento, es decir, la modificación directa del dato almacenado.

Procedimientos seguros de inicio de sesión

Control: Cuando sea requerido por la política de control de accesos se debería controlar el acceso a los sistemas y aplicaciones mediante un procedimiento seguro de log-on

Aplicación: La Organización implementará un procedimiento de acceso a los sistemas y a las aplicaciones, con el fin de minimizar la oportunidad de acceso no autorizado a los mismos.

Este procedimiento, por lo tanto, debe divulgar la mínima información posible acerca del sistema o de la aplicación, a fin de evitar proveer de asistencia innecesaria a un usuario no autorizado.

El procedimiento de identificación deberá:

- Mantener en secreto los identificadores de sistemas o aplicaciones hasta tanto se halla llevado a cabo exitosamente el proceso de conexión.
- Desplegar un aviso general advirtiendo que sólo los usuarios autorizados pueden acceder al equipo.
- Evitar dar mensajes de ayuda que pudieran asistir a un usuario no autorizado durante el procedimiento de conexión.
- Validar la información de la conexión sólo al completarse la totalidad de los datos de entrada. Si surge una condición de error, el sistema no debe indicar que parte de los datos es correcta o incorrecta.
- Limitar el número de intentos de conexión no exitosos permitidos y:
- Registrar los intentos no exitosos.

- Impedir otros intentos de identificación, una vez superado el límite permitido.
- Desconectar conexiones de comunicaciones de datos.
- Limitar el tiempo máximo permitido para el procedimiento de conexión. Si este es excedido, el sistema debe finalizar la conexión.
- Desplegar la siguiente información, al completarse una conexión exitosa:
- Fecha y hora de la conexión exitosa anterior.
- Detalles de los intentos de conexión no exitosos desde la última conexión exitosa.

- Gestión de contraseñas de usuario

Control: Los sistemas de gestión de contraseñas deberían ser interactivos y asegurar contraseñas de calidad.

Aplicación: Las contraseñas constituyen uno de los principales medios de validación de la autoridad de un usuario para acceder a un servicio informático. Los sistemas de administración de contraseñas deben constituir una herramienta eficaz e interactiva que garantice contraseñas de calidad.

El sistema de administración de contraseñas debe:

- Imponer el uso de contraseñas individuales para determinar responsabilidades.
- Permitir que los usuarios seleccionen y cambien sus propias contraseñas (luego de cumplido el plazo mínimo de mantenimiento de las mismas) e incluir un procedimiento de confirmación para contemplar los errores de ingreso.
- Imponer una selección de contraseñas de calidad según lo señalado en el objetivo relativo al uso de información confidencial para la autenticación.
- Imponer cambios en las contraseñas en aquellos casos en que los usuarios mantengan sus propias contraseñas, según lo señalado en el objetivo sobre el uso de información confidencial para la autenticación.
- Obligar a los usuarios a cambiar las contraseñas provisorias en su primer procedimiento de identificación, en los casos en que ellos seleccionen sus contraseñas.
- Mantener un registro de las últimas contraseñas utilizadas por el usuario, y evitar la reutilización de las mismas.
- Evitar mostrar las contraseñas en pantalla, cuando son ingresadas.
- Almacenar en forma separada los archivos de contraseñas y los datos de sistemas de aplicación.
- Modificar todas las contraseñas predeterminadas por el vendedor, una vez instalado el software y el hardware (por ejemplo claves de impresoras, hubs, routers, etc.).

- Garantizar que el medio utilizado para acceder/utilizar el sistema de contraseñas, asegure que no se tenga acceso a información temporal o en tránsito de forma no protegida.

• Uso de herramientas de administración de sistemas

Control: El uso de utilidades software que podrían ser capaces de anular o evitar controles en aplicaciones y sistemas deberían estar restringidos y estrechamente controlados.

Aplicación: La mayoría de los sistemas de información y de las aplicaciones tienen uno o más programas utilitarios que podrían tener la capacidad de pasar por alto los controles de sistemas y aplicaciones. Es esencial que su uso sea limitado y minuciosamente controlado. Se deben considerar los siguientes controles:

- Utilizar procedimientos de autenticación para utilidades del sistema.
- Separar entre utilidades del sistema y software de aplicaciones.
- Limitar el uso de utilidades del sistema a la cantidad mínima viable de usuarios fiables y autorizados.
- Evitar que personas ajenas la Organización tomen conocimiento de la existencia y modo de uso de las utilidades instaladas en las instalaciones informáticas.
- Establecer autorizaciones para el uso apropiado de utilidades de sistema.
- Limitar la disponibilidad de utilidades del sistema, por ejemplo durante el transcurso de un cambio autorizado.
- Registrar todo uso de utilidades del sistema.
- Definir y documentar los niveles de autorización para utilidades del sistema.
- Remover todo el software basado en utilidades y software de sistema innecesarios.

• Control de acceso al código fuente de los programas

Control: Se debería restringir el acceso al código fuente de las aplicaciones software.

Aplicación: Con el fin de minimizar la probabilidad de alteración de programas fuentes, se aplicarán los siguientes controles:

La Organización designará a un funcionario del Departamento de Sistemas como el responsable del código fuente de los programas que tenga la entidad, quien lo tendrá en custodia y deberá:

- Proveer al personal de Desarrollo los programas fuentes solicitados para su modificación, manteniendo en todo momento la correlación programa fuente / ejecutable.

- Llevar un registro actualizado de todos los programas fuentes en uso, indicando nombre del programa, programador, Analista Responsable que autorizó, versión, fecha de última modificación y fecha / hora de compilación y estado (en modificación, en producción).
- Verificar que el Analista Responsable que autoriza la solicitud de un programa fuente sea el designado para la aplicación, rechazando el pedido en caso contrario. Registrar cada solicitud aprobada.
- Administrar las distintas versiones de una aplicación.
- Asegurar que un mismo programa fuente no sea modificado simultáneamente por más de un desarrollador.
- El responsable del código fuente, no tendrá permiso de modificación sobre los programas bajo su custodia.
- Establecer que todo programa objeto o ejecutable en producción tenga un único programa fuente asociado que garantice su origen.
- Establecer que el encargado del desarrollo efectuará la generación del programa objeto o ejecutable que estará en producción (compilación), a fin de garantizar tal correspondencia.
- Desarrollar un procedimiento que garantice que toda vez que se migre a desarrollo el módulo fuente, se cree el código ejecutable correspondiente en forma automática.
- Evitar que la función de responsable del código fuente de los programas, sea ejercida por personal que pertenezca al sector de desarrollo y/o mantenimiento.
- Prohibir la guarda de programas fuentes históricos (que no sean los correspondientes a los programas operativos) en el ambiente de desarrollo.
- Prohibir el acceso a todo operador y/o usuario de aplicaciones a los ambientes y a las herramientas que permitan la generación y/o manipulación de los programas fuentes.
- Realizar las copias de respaldo de los programas fuentes cumpliendo los requisitos de seguridad establecidos por la Organización en los procedimientos que surgen de la presente política.

12.6 CIFRADO

12.6.1 CONTROLES CRIPTOGRÁFICOS

- Política de uso de los controles criptográficos

Control: Se debería desarrollar e implementar una política que regule el uso de controles criptográficos para la protección de la información.

Aplicación: La Organización determina el uso de controles criptográficos en los siguientes casos, previa verificación de que se procede conforme a lo que dicta la Ley:

- Para la protección de claves de acceso a sistemas, datos y servicios.
- Para la transmisión de información clasificada, fuera del ámbito de la Organización.
- Para el resguardo de información, cuando así surja de la evaluación de riesgos realizada por el propietario de la información y el responsable del Departamento de Sistemas designado para tal fin.

El propietario de la información y el responsable del Departamento de Sistemas, harán una evaluación de riesgos de la información, con el fin de determinar el nivel requerido de protección y así mismo el algoritmo de cifrado y la longitud de las claves criptográficas a utilizar.

Con el fin de garantizar la autenticidad y la integridad de los documentos electrónicos, la Organización hará uso de firmas digitales, las cuales previamente han sido gestionadas con la entidad autorizada para ello, en este caso Certicámara Bogotá; el uso de estas firmas no será de uso obligatorio para todos los documentos que procese electrónicamente la Organización, aplicará para todos aquellos cuya información revista mayor importancia para la Organización y para la entidad que recibirá la misma.

Los servicios de no repudio se utilizarán cuando sea necesario resolver disputas acerca de la ocurrencia de un evento o acción. Su objetivo es proporcionar herramientas para evitar que aquél que haya originado una transacción electrónica niegue haberla efectuado.

- Gestión de claves

Control: Se debería desarrollar e implementar una política sobre el uso, la protección y el ciclo de vida de las claves criptográficas a través de todo su ciclo de vida.

Aplicación: La Organización implementará un sistema de administración de claves criptográficas para respaldar la utilización de los dos tipos de técnicas criptográficas, a saber:

- Técnicas de clave secreta (criptografía simétrica), cuando dos o más actores comparten la misma clave y ésta se utiliza tanto para cifrar información como para descifrarla.
- Técnicas de clave pública (criptografía asimétrica), cuando cada usuario tiene un par de claves: una clave pública (que puede ser revelada a cualquier persona) utilizada para cifrar y una clave privada (que debe mantenerse en secreto) utilizada para descifrar. Las claves asimétricas utilizadas para cifrado no deben ser las mismas que se utilizan para firmar digitalmente.

Todas las claves serán protegidas contra modificación y destrucción, y las claves secretas y privadas serán protegidas contra copia o divulgación no autorizada.

Se proporcionará una protección adecuada al equipamiento utilizado para generar, almacenar y archivar claves, considerándolo crítico o de alto riesgo.

SEGURIDAD FÍSICA Y AMBIENTAL

ÁREAS SEGURAS

- Perímetro de seguridad física

Control: Se deberían definir y utilizar perímetros de seguridad para la protección de las áreas que contienen información y las instalaciones de procesamiento de información sensible o crítica.

Aplicación: El Departamento de Sistemas en conjunto con la División Administrativa, definirán las áreas restringidas las cuales se identifican porque allí se almacenan, se procesan o utilizan activos de tecnología e informática, activos considerados como críticos con un grado de confidencialidad

Los responsables de estas áreas igualmente definirán los controles de acceso así como su monitoreo.

- Controles físicos de entrada

Control: Las áreas seguras deberían estar protegidas mediante controles de entrada adecuados para garantizar que solo el personal autorizado dispone de permiso de acceso.

Aplicación: El acceso de personal externo a áreas protegidas se limitará. Este se dará cuando sea necesario y en acompañamiento de personal autorizado.

Se llevará un registro del ingreso y salida del personal del área protegida, identificando hora, fecha (DD/MM/AA), motivos de ingreso, identificación del personal que ingresa así como del acompañante autorizado.

- Seguridad de oficinas, despachos y recursos

Control: Se debería diseñar y aplicar un sistema de seguridad física a las oficinas, salas e instalaciones de la organización.

Aplicación: Dentro de las políticas, lineamientos que defina la Organización para apalancar la Seguridad Informática, definirá:

- La ubicación segura de los equipos de soporte como son las fotocopiadoras y faxes.
- El bloqueo de los equipos de cómputo cuando los usuarios están fuera de su sitio de trabajo.
- Control de movimientos para los equipos portátiles
- Control de utilización de discos duros externos, memorias USB.
- El no consumo de comida y bebidas en el datacenter (centro de servidores) y oficinas.
- Almacenamiento bajo llave de documentos de carácter confidencial y crítico.

- Protección contra las amenazas externas y ambientales

Control: Se debería diseñar y aplicar una protección física contra desastres naturales, ataques maliciosos o accidentes.

Aplicación: La Organización dentro de su programa de prevención y atención y desastres deberá establecer las políticas necesarias para proteger al personal como los activos de información.

Para ello deberá demarcar las zonas seguras así como dotarlas con extintores, igualmente deberá evaluar las condiciones en las que se encuentran estas zonas seguras con el fin de adecuar los diseños en pro de evitar inundaciones y/o riesgos eléctricos.

Se deberá concientizar y promover por medio de capacitaciones la importancia de proteger estos activos, y el valor que tiene que todos contribuyan a la protección de los mismos.

- El trabajo en áreas seguras

Control: Se deberían diseñar y aplicar procedimientos para el desarrollo de trabajos y actividades en áreas seguras.

Aplicación: La protección física de las áreas seguras, se fortalece estableciendo barreras físicas y de acceso a estas áreas, para ello la Organización define como lineamiento que:

- Ningún funcionario deberá permanecer en un área segura fuera del horario normal de trabajo.
- Los accesos a las zonas restringidas deberán ser controlados y asignados de acuerdo a sus roles y responsabilidades.
- Las zonas identificadas como restringidas deberán contar con extintores y equipo que permita controlar incidentes como incendios.

- Áreas de acceso público, carga y descarga

Control: Se deberían controlar puntos de acceso a la organización como las áreas de entrega y carga/descarga (entre otros) para evitar el ingreso de personas no autorizadas a las dependencias aislando estos puntos, en la medida de lo posible, de las instalaciones de procesamiento de información.

Aplicación: Para evitar incidentes en las zonas seguras de la Organización se debe:

- Inspeccionar y registrar las cargas antes de entrar al edificio para evitar potenciales amenazas.
- Las zonas de carga, despacho y acceso al público deben ser zonas incomunicadas con las zonas seguras, para evitar el acceso a personal no autorizado.

12.7 SEGURIDAD DE LOS EQUIPOS

- Emplazamiento y protección de equipos

Control: Los equipos se deberían emplazar y proteger para reducir los riesgos de las amenazas y peligros ambientales y de oportunidades de acceso no autorizado.

Aplicación: Con el fin de proteger los equipos y mantener su vida útil se implementarán los siguientes lineamientos:

- Se establecerán normas para el consumo de alimentos en los puestos de trabajo.
- Se realizará monitoreo permanente al ambiente con el fin de mantener las temperaturas adecuadas a cada uno de los centros de procesamiento.
- Ubicar los equipos de cómputo de tal forma que se impida que la información sea visible por terceros.

- Instalaciones de suministro

Control: Los equipos deberían estar protegidos contra cortes de luz y otras interrupciones provocadas por fallas en los suministros básicos de apoyo.

Aplicación: Dentro de la Organización existen servicios de suministro que soportan todo el procesamiento de información como son el servicio de energía, respaldo con UPS, equipos de comunicación entre otros.

Para ello es necesario que estos servicios se estén monitoreando y realizando mantenimiento preventivo para identificar fallas y corregirlas, y así mitigar los impactos que la no prestación de estos servicios pudiera ocasionar en los servicios de procesamiento con los cuales hoy cuenta la Organización.

- Seguridad del cableado

Control: Los cables eléctricos y de telecomunicaciones que transportan datos o apoyan a los servicios de información se deberían proteger contra la intercepción, interferencia o posibles daños.

Aplicación: El cableado estructurado de la Organización debe estar diseñado de tal forma que soporte los servicios tecnológicos y de comunicaciones que requiere, su diseño debe estar documentado de tal forma que se identifique la topología, los puntos, la categoría de los cables y la tecnología utilizada. Dentro de esta estructura se debe definir que la alimentación eléctrica debe estar separada del cableado estructurado con el fin de evitar interferencias.

- Mantenimiento de los equipos

Control: Los equipos deberían mantenerse adecuadamente con el objeto de garantizar su disponibilidad e integridad continuas.

Aplicación: Garantizar que todos los componentes de Hardware y Software de la entidad reciban un adecuado mantenimiento preventivo y correctivo de tal manera que los procesos normales de la entidad no se vean afectados por fallas en los equipos de cómputo.

El mantenimiento preventivo debe definirse dentro de un cronograma donde se establezca la ubicación del equipo y la clase de mantenimiento que se le hará, si es físico y/o lógico.

El personal que realice los mantenimientos debe ser capacitado y autorizado, ya que tiene acceso a información sensible, pública, restringida, la cual debe conservar y proteger mientras elabora estas actividades.

Dentro de las hojas de vida de cada equipo se debe consignar la novedad de mantenimiento realizada de forma detallada, igualmente llevará libro de bitácora para registrar los mantenimientos realizados según cronograma.

- Salida de activos fuera de las dependencias de la empresa

Control: Los equipos, la información o el software no se deberían retirar del sitio sin previa autorización.

Aplicación: para retirar activos de información físicos deberá contar con la autorización del Departamento de Sistemas y del área de Auditoría Interna quien controla los inventarios dentro de la Organización. Dentro del registro se deberán identificar los datos del responsable, el motivo del retiro del activo y el destino.

Los activos de información lógicos (software) sólo los retirará el personal autorizado del Departamento de Sistemas, ya que ellos tienen los accesos y la formación necesaria para realizar esta actividad, ellos deberán registrar la identificación del activo, el motivo del retiro del activo y la máquina de donde fue retirado el activo, esto con el fin de mantener actualizado el inventario de activos de la Organización.

- Seguridad de los equipos y activos fuera de las instalaciones

Control: Se debería aplicar la seguridad a los activos requeridos para actividades fuera de las dependencias de la organización y en consideración de los distintos riesgos.

Aplicación: dentro y fuera de las instalaciones de la Organización, el responsable del equipo deberá velar por la seguridad de éste, para ello se seguirán los siguientes lineamientos:

- La Organización deberá contar con seguros que protejan los equipos.
- Registro de ingreso y salida de las instalaciones de la Organización.
- Los equipos portátiles siempre deberán llevarse como equipaje de mano.
- El responsable del equipo no permitirá que este sea manipulado por un tercero no autorizado, tampoco lo desatenderá ni mucho menos lo dejará a la vista en un lugar público.
- En caso de presentarse robo, deberá instaurar la denuncia ante la autoridad competente e informar al jefe de área o unidad, según corresponda, para iniciar los trámites internos a los que hubiese lugar.

- Reutilización o retirada segura de dispositivos de almacenamiento

Control: Se deberían verificar todos los equipos que contengan medios de almacenamiento para garantizar que cualquier tipo de datos sensibles y software con licencia se hayan extraído o se hayan sobrescrito de manera segura antes de su eliminación o reutilización.

Aplicación: Antes de dar de baja un equipo o reasignarlo, se debe eliminar la información sensible que este contenga, con el fin de evitar la pérdida de la información y recuperación de información no autorizada, igualmente se debe

desinstalar cualquier software, de tal forma que se evite tener problemas de licenciamiento.

- Equipo informático de usuario desatendido

Control: Los usuarios se deberían asegurar de que los equipos no supervisados cuentan con la protección adecuada.

Aplicación: Los usuarios deberán garantizar que los equipos desatendidos sean protegidos adecuadamente.

Todos los equipos que posee la Organización, sean los instalados en los puestos de trabajo o los ubicados en el centro de procesamiento de los datos, requieren protección específica frente a acceso no autorizado cuando se encuentran desatendidos.

La Organización proporcionará las pautas para que los usuarios y el personal externo que se encuentre en labores para la entidad, protejan sus equipos cuando estén ausentes de sus puestos de trabajo; de igual manera se encargará de verificar el cumplimiento de las mismas. Dichas pautas son:

- Concluir las sesiones activas al finalizar las tareas, a menos que puedan protegerse mediante un mecanismo de bloqueo adecuado, por ejemplo, un protector de pantalla protegido por contraseña.
- Proteger los computadores contra usos no autorizados mediante un bloqueo de seguridad o control equivalente, por ejemplo, contraseña de acceso cuando no se utilizan.

- Política de puesto de trabajo despejado y bloqueo de pantalla

Control: Se debería adoptar una política de puesto de trabajo despejado para documentación en papel y para medios de almacenamiento extraíbles y una política de monitores sin información para las instalaciones de procesamiento de información.

Aplicación: La Organización adoptará una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.

Se aplicarán los siguientes lineamientos:

- Almacenar bajo llave, cuando corresponda, los documentos en papel y los medios informáticos, en gabinetes y/u otro tipo de mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.
- Guardar bajo llave la información sensible o crítica de la organización (preferentemente en una Organización fuerte o gabinete a prueba de incendios) cuando no está en uso, especialmente cuando no hay personal en la oficina.
- Desconectar de la red / sistema / servicio los computadores personales, terminales e impresoras asignadas a funciones críticas, cuando están desatendidas. Las mismas deben ser protegidas mediante cerraduras de seguridad, contraseñas u otros controles cuando no están en uso (como por ejemplo la utilización de protectores de pantalla con contraseña). Los responsables de cada área mantendrán un registro de las contraseñas o copia de las llaves de seguridad utilizadas en el sector a su cargo. Tales elementos se encontrarán protegidos en sobre cerrado o de seguridad para impedir accesos no autorizados, debiendo dejarse constancia de todo acceso a las mismas, y de los motivos que llevaron a tal acción.
- Proteger los puntos de recepción y envío de correo postal y las máquinas de fax no atendidas.
- Bloquear las fotocopiadoras (o protegerlas de alguna manera del uso no autorizado) fuera del horario normal de trabajo.
- Retirar inmediatamente la información sensible o confidencial, una vez impresa.

12.8 SEGURIDAD OPERATIVA

12.8.1 RESPONSABILIDADES Y PROCEDIMIENTOS DE OPERACIÓN

- Documentación de procedimientos de operación

Control: Se deberían documentar los procedimientos operativos y dejar a disposición de todos los usuarios que los necesiten.

Aplicación: La Organización a través de su Departamento de Sistemas, documentará y mantendrá actualizados los procedimientos operativos identificados en ésta política, los cuales deben ser solicitados por el área que los requiera y autorizados por el Departamento de Sistemas.

Los procedimientos especificarán instrucciones para la ejecución detallada de cada tarea, incluyendo:

Procesamiento y manejo de la información.
Requerimientos de programación de procesos, interdependencias con otros sistemas, tiempos de inicio de las primeras tareas y tiempos de terminación de las últimas tareas.

Instrucciones para el manejo de errores u otras condiciones excepcionales que puedan surgir durante la ejecución de tareas.
Restricciones en el uso de utilidades del sistema.
Personas de soporte a contactar en caso de dificultades operativas o técnicas imprevistas.
Instrucciones especiales para el manejo de “salidas”, como el uso de papelería especial o la administración de salidas confidenciales, incluyendo procedimientos para la eliminación segura de salidas fallidas de tareas.
Reinicio del sistema y procedimientos de recuperación en caso de producirse fallas en el sistema.

Se preparará adicionalmente documentación sobre procedimientos referidos a las siguientes actividades:

- Instalación y mantenimiento de equipamiento para el procesamiento de información y comunicaciones.
- Instalación y mantenimiento de las plataformas de procesamiento.
- Monitoreo del procesamiento y las comunicaciones.
- Inicio y finalización de la ejecución de los sistemas.
- Programación y ejecución de procesos.
- Gestión de servicios.
- Resguardo de información.
- Gestión de incidentes de seguridad en el ambiente de procesamiento y comunicaciones.
- Reemplazo o cambio de componentes del ambiente de procesamiento y comunicaciones.
- Uso del correo electrónico.
- Gestión de cambios

Control: Se deberían controlar los cambios que afectan a la Seguridad Informática en la organización y procesos de negocio, las instalaciones y sistemas de procesamiento de información.

Aplicación: Se definirán procedimientos para el control de los cambios en el ambiente operativo y de comunicaciones. Todo cambio deberá ser evaluado previamente en aspectos técnicos y de seguridad.

El Departamento de Sistemas controlará que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de los mismos ni de la información que soportan, ni afecte la operación de los sistemas. Dicho departamento velará por la correcta implementación de los mismos.

Se tendrá un registro que contenga toda la información relevante de cada cambio implementado.

Los procedimientos de control de cambios contemplarán los siguientes puntos:

Identificación y registro de cambios significativos.

- Evaluación del posible impacto de dichos cambios.
- Aprobación formal de los cambios propuestos.
- Planificación del proceso de cambio.
- Prueba del nuevo escenario.
- Comunicación de detalles de cambios a todas las personas pertinentes.
- Identificación de las responsabilidades por la cancelación de los cambios fallidos y la recuperación respecto de los mismos.

- Gestión de capacidades

Control: Se debería monitorear y ajustar el uso de los recursos junto a proyecciones necesarias de requisitos de capacidad en el futuro con el objetivo de garantizar el rendimiento adecuado en los sistemas.

Aplicación: El Departamento de Sistemas realizará monitoreo y análisis permanente a toda la infraestructura tecnológica de procesamiento de información, con el fin de identificar el estado y la utilización de todos los recursos.

Con esto se busca optimizar los recursos existentes, y vislumbrar las proyecciones de crecimiento, con el fin de identificar las necesidades y asegurar que la infraestructura esté en las condiciones necesarias para atender la demanda existente y la futura.

- Separación de entornos de desarrollo, prueba y producción

Control: Los entornos de desarrollo, pruebas y operacionales deberían permanecer separados para reducir los riesgos de acceso o de cambios no autorizados en el entorno operacional.

Aplicación: Con el fin de garantizar la integridad de la información, es necesario que la Organización cuente con tres ambientes para la ejecución de actividades, se recomienda que la separación de los ambientes sea física, de lo contrario, los accesos a cada uno de los directorios debe ser bajo control de accesos y continuamente monitoreados.

Se propone que los ambientes que deben estar disponibles son:

Ambiente de producción: Recursos informáticos que soporta las aplicaciones existentes en la Organización y que utilizan a diario por cada uno de los funcionarios de la misma.

Ambiente de desarrollo: Recursos informáticos necesarios para la generación y modificación de aplicaciones, así como su análisis y programación, con este ambiente se previenen problemas operativos.

Ambiente de pruebas: Recursos informáticos que soportan la verificación de funcionalidades de las aplicaciones que fueron desarrolladas para paso a producción.

Con la separación de ambientes se logra:

- Asegurar un mayor control.
- Incrementar el control a las versiones fuentes de desarrollo.
- Asegurar el acceso autorizado a los programas fuentes.

12.8.2 PROTECCIÓN CONTRA CÓDIGO MALICIOSO

- Controles contra el código malicioso

Control: Se deberían implementar controles para la detección, prevención y recuperación ante afectaciones de malware en combinación con la concientización adecuada de los usuarios.

Aplicación: El Departamento de Sistemas definirá e implementará controles de detección y prevención para la protección contra software malicioso.

El Departamento de Sistemas desarrollará procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.

Estos controles deberán considerar las siguientes acciones:

- Prohibir el uso de software no autorizado
- Redactar procedimientos para evitar los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas, o por cualquier otro medio, señalando las medidas de protección a tomar.
- Instalar y actualizar periódicamente software de detección y reparación de virus, examinado computadores y medios informáticos, como medida de precaución y rutinaria.
- Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles (probar dichas actualizaciones en un entorno de prueba previamente si es que constituyen cambios críticos a los sistemas).
- Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos de la Organización, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.

- Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.
- Redactar procedimientos para verificar toda la información relativa a software malicioso, garantizando que los boletines de alerta sean exactos e informativos.
- Concientizar al personal acerca del problema de los falsos virus (hoax) y de cómo proceder frente a los mismos.

12.8.3 COPIAS DE SEGURIDAD

- Copias de Seguridad Informática

Control: Se deberían realizar y pruebas regulares de las copias de la información, del software y de las imágenes del sistema en relación a una política de respaldo (Backup) convenida.

Aplicación: La Organización debe asegurar que los datos de los usuarios y clientes se mantengan protegidos contra pérdidas, alteración o divulgación por actos accidentales o malintencionados o por fallas de los equipos y/o redes.

Para ello, deberá definir lineamientos para realizar las copias de seguridad a los servidores y bases de datos que soportan los activos de información de la Organización.

Dentro de los lineamientos que defina debe ser explicita en indicar la periodicidad con que se deben realizar las copias, definir el tiempo en que se realizara la copia (hora), los dispositivos de almacenamiento, la identificación que debe llevar cada copia, el lugar de almacenamiento, la responsabilidad de realizar las copias así como sus actualizaciones por evolución de tecnología, definición de tiempo de conservación.

12.8.4 REGISTRO DE ACTIVIDAD Y SUPERVISIÓN

- Registro y gestión de eventos de actividad

Control: Se deberían producir, mantener y revisar periódicamente los registros relacionados con eventos de actividad del usuario, excepciones, fallas y eventos de Seguridad Informática.

Aplicación: Se generarán registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad.

Los registros de auditoría deberán incluir:

- Identificación del usuario.
- Fecha y hora de inicio y terminación.
- Identidad o ubicación del equipo, si se hubiera dispuesto identificación automática para la misma.
- Registros de intentos exitosos y fallidos de acceso al sistema.
- Registros de intentos exitosos y fallidos de acceso a datos y otros recursos.

En todos los casos, los registros de auditoría serán archivados preferentemente en un equipo diferente al que los genere y conforme los requerimientos del objetivo recopilación de evidencias.

El propietario de la información junto con el área de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad Informática, definirá un cronograma de depuración de registros en línea en función a normas vigentes y a sus propias necesidades.

- Protección de los registros de información

Control: Se debería proteger contra posibles alteraciones y accesos no autorizados la información de los registros.

Aplicación: El Departamento de Sistemas y los propietarios de la información determinarán los requerimientos para resguardar cada software o dato en función de su criticidad. En base a ello, se definirá y documentará un esquema de resguardo de la información.

El Departamento de Sistemas dispondrá y controlará la realización de dichas copias, así como la prueba periódica de su restauración. Para esto se deberá contar con instalaciones de resguardo que garanticen la disponibilidad de toda la información y del software crítico de la Organización. Los sistemas de resguardo deberán probarse periódicamente, asegurándose que cumplen con los requerimientos de los planes de continuidad de las actividades de la entidad, según el objetivo: Verificación, revisión y evaluación de la continuidad de la Seguridad Informática.

Se definirán procedimientos para el resguardo de la información, que deberán considerar los siguientes puntos:

Definir un esquema de rótulo de las copias de resguardo, que permita contar con toda la información necesaria para identificar cada una de ellas y administrarlas debidamente.
Establecer un esquema de reemplazo de los medios de almacenamiento de las copias de resguardo, una vez concluida la posibilidad de ser reutilizados, de acuerdo a lo indicado por el proveedor, y asegurando la destrucción de los medios

desechados. (Ver objetivo: Reutilización o retirada segura de dispositivos de almacenamiento).
Almacenar en una ubicación remota copias recientes de información de resguardo junto con registros exactos y completos de las mismas y los procedimientos documentados de restauración, a una distancia suficiente como para evitar daños provenientes de un desastre en el sitio principal. Se deberán retener al menos tres generaciones o ciclos de información de resguardo para la información y el software esenciales para la Organización. Para la definición de información mínima a ser resguardada en el sitio remoto, se deberá tener en cuenta el nivel de clasificación otorgado a la misma, en términos de disponibilidad (Ver objetivo CLASIFICACIÓN DE LA INFORMACIÓN) y requisitos legales a los que se encuentre sujeta.

- Asignar a la información de resguardo un nivel de protección física y ambiental según las normas aplicadas en el sitio principal. Extender los mismos controles aplicados a los dispositivos en el sitio principal al sitio de resguardo.
- Probar periódicamente los medios de resguardo.
- Verificar y probar periódicamente los procedimientos de restauración garantizando su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procedimientos operativos.

Los procedimientos de realización de copias de resguardo y su almacenamiento deberán respetar las disposiciones de los objetivos CLASIFICACIÓN DE LA INFORMACIÓN y Protección de los registros de la organización.

- Registros de actividad del administrador y operador del sistema

Control: Se deberían registrar las actividades del administrador y del operador del sistema y los registros asociados se deberían proteger y revisar de manera regular.

Aplicación: El Departamento de Sistemas asegurará el registro de las actividades realizadas en los sistemas, incluyendo según corresponda:

- Tiempos de inicio y cierre del sistema.
- Errores del sistema y medidas correctivas tomadas.
- Intentos de acceso a sistemas, recursos o información crítica o acciones restringidas
- Ejecución de operaciones críticas
- Cambios a información crítica

El área de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad Informática contrastará los registros de actividades del personal operativo con relación a los procedimientos operativos.

- Sincronización de relojes

Control: Se deberían sincronizar los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o de un dominio de seguridad y en relación a una fuente de sincronización única de referencia.

Aplicación: A fin de garantizar la exactitud de los registros de auditoría, al menos los equipos que realicen estos registros, deberán tener una correcta configuración de sus relojes.

Para ello, se dispondrá de un procedimiento de ajuste de relojes, el cual indicará también la verificación de los relojes contra una fuente externa del dato y la modalidad de corrección ante cualquier variación significativa.

12.8.5 CONTROL DEL SOFTWARE EN EXPLOTACIÓN

- Instalación del software en sistemas en producción

Control: Se deberían implementar procedimientos para controlar la instalación de software en sistemas operacionales.

Aplicación: Los procesos de instalación, desinstalación, actualización y/o modificación de software deberán ser realizados únicamente por el personal del Departamento de Sistemas; ningún usuario que no pertenezca a dicho departamento está autorizado para realizar ninguna de las anteriores gestiones sobre el software.

Cualquier requerimiento que implique la modificación o cambio de software, deberá ser solicitado directamente al Departamento de Sistemas de la Organización. Dichos requerimientos deberán ser debidamente documentados por el área encargada con el fin de soportar los cambios realizados, a efectos de auditorías internas.

12.8.6 GESTIÓN DE LA VULNERABILIDAD TÉCNICA

- Gestión de las vulnerabilidades técnicas

Control: Se debería obtener información sobre las vulnerabilidades técnicas de los sistemas de información de manera oportuna para evaluar el grado de exposición de la organización y tomar las medidas necesarias para abordar los riesgos asociados.

Aplicación: A fin de tener información referente a las vulnerabilidades técnicas de los sistemas de información existentes en la Organización, la misma establecerá un procedimiento para la controlar las vulnerabilidades técnicas, el cual deberá:

- Contar con un inventario detallado y actualizado de los activos de información, separados por tipos de activos (software, hardware, datos, redes de comunicación, etc.)
- Disponer de fuentes de información técnica que informen sobre las vulnerabilidades descubiertas.
- Realizar un análisis detallado a sus activos de información con el fin de identificar posibles vulnerabilidades, no incluidas dentro de las reconocidas públicamente, a fin de evaluar la exposición de la Organización ante dichas amenazas para definir y aplicar las acciones apropiadas para mitigar el impacto sobre la entidad.
- Realizar revisiones periódicas a las acciones existentes para mitigar el impacto de las amenazas ocasionadas por las vulnerabilidades identificadas, a fin de evaluar si esas acciones son eficaces y efectivas o si por el contrario requieren ajustes o cambios. Dichas revisiones deben quedar debidamente documentadas, y dichos soportes debidamente guardados, como material de consulta para futuras acciones a emprender por parte de la Organización.

    - Restricciones en la instalación de software

Control: Se deberían establecer e implementar las reglas que rigen la instalación de software por parte de los usuarios.

Aplicación: El Área de Sistemas es la responsable de la instalación de los programas de software en cada uno de los computadores de la Organización; por tanto no está permitido que los usuarios realicen instalaciones de cualquier tipo de software en sus computadoras. De requerir un software específico debe solicitarse al Área de Sistemas para que se valore la necesidad de su instalación.

Todo software que se instale en los computadores de la Organización deberá contar con su respectiva licencia y su instalación deberá ser autorizada por la jefatura del Área de Sistemas

No está permitida la instalación del software adquirido por la Organización en equipos que no sean de su propiedad

12.8.7 CONSIDERACIONES DE LAS AUDITORÍAS DE LOS SISTEMAS DE INFORMACIÓN

- Controles de auditoría de los sistemas de información

Control: Se deberían planificar y acordar los requisitos y las actividades de auditoría que involucran la verificación de los sistemas operacionales con el objetivo de minimizar las interrupciones en los procesos relacionados con el negocio.

Aplicación: La realización de actividades de auditoría que involucren verificaciones de los sistemas en producción, implican una planificación de los requerimientos y tareas, a fin de minimizar el riesgo de interrupción en las operaciones de las áreas involucradas en la auditoría.

Para tal efecto se tendrá en cuenta lo siguiente:

- Acordar con el Área que corresponda los requerimientos de auditoría.
- Controlar el alcance de las verificaciones. Esta función será realizada por el responsable de auditoría.
- Limitar las verificaciones a un acceso de sólo lectura del software y datos de producción. Caso contrario, se tomarán las contramedidas necesarias a fin de aislar y contrarrestar los efectos de las modificaciones realizadas, una vez finalizada la auditoría. Por ejemplo:
- Eliminar archivos transitorios.
- Eliminar entidades ficticias y datos incorporados en archivos maestros.
- Revertir transacciones.
- Revocar privilegios otorgados
- Identificar claramente los recursos necesarios para llevar a cabo las verificaciones, los cuales serán puestos a disposición de los auditores.
- Identificar y acordar los requerimientos de procesamiento especial o adicional.
- Monitorear y registrar todos los accesos, a fin de generar una pista de referencia. Los datos a resguardar deben incluir como mínimo:
- Fecha y hora.
- Puesto de trabajo.
- Usuario.
- Tipo de acceso.
- Identificación de los datos accedidos.
- Estado previo y posterior.
- Programa y/o función utilizada.
- Documentar todos los procedimientos de auditoría, requerimientos y responsabilidades.

12.9 SEGURIDAD EN LAS TELECOMUNICACIONES

12.9.1 GESTIÓN DE LA SEGURIDAD EN LAS REDES

- Controles de red

Control: Se deberían administrar y controlar las redes para proteger la información en sistemas y aplicaciones.

Aplicación: El Departamento de Sistemas definirá e implementará controles para garantizar la seguridad de los datos y los servicios conectados en las redes de la entidad, contra el acceso no autorizado, considerando la ejecución de las siguientes acciones:

- Establecer los procedimientos para la administración del equipamiento remoto, incluyendo los equipos en las áreas usuarias, el cual será llevado a cabo por el responsable establecido en el objetivo de Responsabilidades y procedimientos.
- Establecer controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados.
- Implementar controles especiales para mantener la disponibilidad de los servicios de red y computadores conectados.
- Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información.

    - Mecanismos de seguridad asociados a servicios en red

Control: Se deberían identificar e incluir en los acuerdos de servicio (SLA) los mecanismos de seguridad, los niveles de servicio y los requisitos de administración de todos los servicios de red, independientemente de si estos servicios se entregan de manera interna o están externalizados.

Aplicación: El Departamento de Sistemas definirá las pautas para garantizar la seguridad de los servicios de red de la Organización, tanto públicos como privados.

Para ello se tendrán en cuenta las siguientes directivas:

- Mantener instalados y habilitados sólo aquellos servicios que sean utilizados.
- Controlar el acceso lógico a los servicios, tanto a su uso como a su administración.
- Configurar cada servicio de manera segura, evitando las vulnerabilidades que pudieran presentar.
- Instalar periódicamente las actualizaciones de seguridad.

Dicha configuración será revisada periódicamente por el Departamento de Sistemas.

- Segregación de redes

Control: Se deberían segregar las redes en función de los grupos de servicios, usuarios y sistemas de información.

Aplicación: Para controlar la seguridad en la red de la Organización, se podrán dividir en dominios lógicos separados. Para esto se definirán y documentarán los perímetros de seguridad que sean convenientes. Estos perímetros se implementarán mediante la instalación de "gateways" con funcionalidades de "firewall" o redes privadas virtuales, para filtrar el tráfico entre los dominios (ver los objetivos 11.4.6. Control de conexión a las redes y 11.4.7. Control de enrutamiento en la red) y para bloquear el acceso no autorizado de acuerdo al objetivo 9.1.1 Política de control de accesos.

La subdivisión en dominios de la red tomará en cuenta criterios como los requerimientos de seguridad comunes de grupos de integrantes de la red, la mayor exposición de un grupo a peligros externos, separación física, u otros criterios de aglutinamiento o segregación preexistentes.

Basándose en la Política de control de acceso y los requerimientos de acceso, el Departamento de Sistemas evaluará el costo relativo y el impacto en el desempeño que ocasione la implementación de enrutadores o gateways adecuados para subdividir la red, para definir el esquema más apropiado a implementar.

12.9.2 INTERCAMBIO DE INFORMACIÓN CON PARTES EXTERNAS

- Políticas y procedimientos de intercambio de información

Control: Deberían existir políticas, procedimientos y controles formales de transferencia para proteger la información que viaja a través del uso de todo tipo de instalaciones de comunicación.

Aplicación: La Organización tendrá un procedimiento frente al intercambio de información con otras organizaciones, regido bajo las políticas de acceso a la información, Seguridad Informática, clasificación de la información, de tal modo que ese intercambio de información no afecte ni las operaciones ni la integridad e imagen de la Organización, ni la integridad e imagen de las empresas y personas de las cuales la Organización tiene en custodia su información.

- Acuerdos de intercambio

Control: Los acuerdos deberían abordar la transferencia segura de información comercial entre la organización y las partes externas.

Aplicación: Cuando se realicen acuerdos entre organizaciones para el intercambio de información y software, se especificarán el grado de sensibilidad de la información de la entidad involucrada y las consideraciones de seguridad sobre la misma. Se tendrán en cuenta los siguientes aspectos:

- Responsabilidades gerenciales por el control y la notificación de transmisiones, envíos y recepciones.
- Procedimientos de notificación de emisión, transmisión, envío y recepción.
- Normas técnicas para el empaquetado y la transmisión.
- Pautas para la identificación del prestador del servicio de correo.
- Responsabilidades y obligaciones en caso de pérdida de datos.
- Uso de un sistema convenido para el rotulado de información clasificada, garantizando que el significado de los rótulos sea inmediatamente comprendido y que la información sea adecuadamente protegida.
- Información sobre la propiedad de la información suministrada y las condiciones de su uso.
- Normas técnicas para la grabación y lectura de la información.
- Controles especiales que puedan requerirse para proteger ítems sensibles, (claves criptográficas, etc.).

    - Mensajería electrónica

Control: Se debería proteger adecuadamente la información referida en la mensajería electrónica.

Aplicación: El Departamento de Sistemas definirá y documentará normas y procedimientos claros con respecto al uso del correo electrónico, que incluya al menos los siguientes aspectos:

- Protección contra ataques al correo electrónico, por ejemplo virus, intercepción, etc.
- Protección de archivos adjuntos de correo electrónico.
- Uso de técnicas criptográficas para proteger la confidencialidad e integridad de los mensajes electrónicos (ver el objetivo CONTROLES CRIPTOGRÁFICOS).
- Retención de mensajes que, si se almacenaran, pudieran ser usados en caso de litigio.
- Controles adicionales para examinar mensajes electrónicos que no pueden ser autenticados.
- Aspectos operativos para garantizar el correcto funcionamiento del servicio (ej.: tamaño máximo de información transmitida y recibida, cantidad de destinatarios, tamaño máximo del buzón del usuario, etc.).

- Definición de los alcances del uso del correo electrónico por parte del personal de la Organización.
- Potestad de la Organización para auditar los mensajes recibidos o emitidos por los servidores la Organización, lo cual se incluirá en el objetivo Acuerdos de confidencialidad y secreto.

Entender al correo electrónico como una herramienta más de trabajo provista al empleado a fin de ser utilizada conforme el uso al cual está destinada, faculta al empleador a implementar sistemas de controles destinados a velar por la protección y el buen uso de sus recursos.

Esta facultad, sin embargo, deberá ejercerse salvaguardando la dignidad del trabajador y su derecho a la intimidad. Por tal motivo, la Organización debe informar claramente a sus empleados: a) cuál es el uso que la entidad espera que los empleados hagan del correo electrónico provisto por la Organización; y b) bajo qué condiciones los mensajes pueden ser objeto de control y monitoreo.

- Acuerdos de confidencialidad y secreto

Control: se deberían identificar, revisar y documentar de manera regular los requisitos para los acuerdos de confidencialidad y "no divulgación" que reflejan las necesidades de la organización para la protección de información.

Aplicación: La Organización deberá elaborar acuerdos de confidencialidad que deberán ser aceptados por el personal que labora en la entidad, este debe reflejar el compromiso de protección y el buen uso de la información.

El acuerdo de confidencialidad debe comenzar a regir desde el mismo momento en que se firma el contrato laboral y permanecerá vigente durante el periodo de duración del contrato, manteniéndose inclusive durante las prórrogas sin necesidad de firmar un nuevo acuerdo de confidencialidad.

Dentro del acuerdo se deberá reconocer que una condición de esta relación laboral consiste en que no usará en el desempeño de sus deberes en la Organización cualquier información propietaria o confidencial de una antigua empresa sin la autorización escrita de aquella entidad.

Igualmente se deberá comprometer que la información entregada por La Organización para el desarrollo de sus labores es confidencial y que cualquier producción que realice durante la ejecución del contrato le pertenece a la Organización.

12.10 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

12.10.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

- Análisis y especificación de los requisitos de seguridad

Control: Los requisitos relacionados con la Seguridad Informática se deberían incluir en los requisitos para los nuevos sistemas o en las mejoras a los sistemas de información ya existentes.

Aplicación: Esta política aplica para incorporar controles de seguridad a los sistemas no sólo desarrollados por la misma Organización, sino también por aquellos que sean adquiridos a terceros, al igual que para las mejoras o actualizaciones que se realicen a los sistemas ya existentes.

Durante las etapas de análisis y diseño del sistema, se incluirán los requerimientos y respectivos controles de seguridad, los cuales serán definidos en conjunto por las áreas usuarias del sistema, el Departamento de Sistemas y Auditoría Interna, quienes determinarán inicialmente las posibles amenazas y posteriormente los controles y/o acciones (manuales o automatizadas) para mitigar los riesgos a los que está expuesto el sistema.

La evaluación de los requerimientos de seguridad debe incluir un análisis costo - beneficio, frente a la implementación de acciones de seguridad en el bien que se quiere proteger y frente al daño potencial que pudiera ocasionar a las actividades realizadas.

Es importante tener en cuenta que incluir acciones de seguridad durante la etapa de análisis y diseño del sistema, es significativamente menos costoso que hacerlo en un sistema que se encuentra en marcha.

- Seguridad de las comunicaciones en servicios accesibles por redes públicas

Control: La información de los servicios de aplicación que pasa a través de redes públicas se debería proteger contra actividades fraudulentas, de disputa de contratos y/o de modificación no autorizada.

Aplicación: Para efectos de los servicios de aplicación que pasan a través de redes públicas, la Organización implementará un procedimiento, que incluya la aplicación de las políticas de Seguridad Informática implantadas en la entidad, mediante el cual se garantice la protección de la información, se verifique la autenticidad y confiabilidad de la “entidad” con la que se esté haciendo el vínculo comercial, además de ajustarse a lo establecido en la legislación del país que rige este tipo de operaciones, como lo es la Ley 527 de 1999.

- Protección de las transacciones por redes telemáticas

Control: La información en transacciones de servicios de aplicación se debería proteger para evitar la transmisión y enrutamiento incorrecto y la alteración, divulgación y/o duplicación no autorizada de mensajes o su reproducción.

Aplicación: Al igual que con los servicios de aplicación que pasan a través de redes públicas, la Organización aplicará de manera estricta todas las políticas de Seguridad Informática definidas al interior de la entidad, con el fin de velar por la integridad de la misma, realizando operaciones en línea bajo los parámetros de integridad, confiabilidad y seguridad, evitando a toda costa cualquier posible fraude o intrusión sin autorización a la información vital de la Organización.

Para garantizar transacciones por redes telemáticas seguras, es relevante tener en cuenta lo siguiente:

- No acceder a sitios de comercio electrónico o internet banking desde computadores de terceros; utilizar siempre un computador personal con antivirus y asegurarse de que la dirección que se presenta en su browser corresponde al sitio que realmente se quiere visitar.
- No utilizar links en páginas de terceros o recibidos vía email y asegurarse de que el sitio tenga una conexión segura, es decir, que los datos transmitidos entre el browser y el sitio están encriptados.
- Configurar el programa de e-mail para que no ejecute programas automáticamente.
- No realizar transacciones con empresas que solicitan un depósito y no dan la opción de pagar con tarjeta de crédito.
- Realizar transacciones sólo en sitios de instituciones que se consideren confiables, dando preferencia a las empresas grandes y conocidas.
- Nunca digitar la clave o datos personales en emails, aunque se hayan recibido de la empresa.

12.10.2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE

- Política de desarrollo seguro de software

Control: Se deberían establecer y aplicar reglas para el desarrollo de software y sistemas dentro de la organización.

Aplicación: La Organización velará porque el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad esperados, con las buenas prácticas para desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado. Además, se asegurará que todo software desarrollado o adquirido,

interna o externamente cuenta con el nivel de soporte requerido por la Organización.

- Procedimientos de control de cambios en los sistemas

Control: En el ciclo de vida de desarrollo se deberían hacer uso de procedimientos formales de control de cambios.

Aplicación: Con el fin de minimizar los riesgos de alteración de los sistemas de información, la Organización implementará procedimientos para la implementación de cambios que se ajusten a las políticas establecidas por la misma; dichos procedimientos deben incluir:

- Verificar que los cambios en las aplicaciones sean propuestos por usuarios autorizados, los cuales deben atender a las políticas establecidas por la Organización y a las licencias de uso.
- Mantener un registro de los niveles de autorización acordados.
- Solicitar la autorización del propietario de la información, en caso de tratarse de cambios a sistemas de procesamiento de la misma.
- Identificar todos los elementos que requieren modificaciones (software, bases de datos, hardware).
- Revisar los controles y los procedimientos de integridad para garantizar que no serán comprometidos por los cambios.
- El Departamento de Sistemas aprobará las tareas necesarias para la gestión de los cambios, antes de que éstas inicien.
- El Departamento de Sistemas deberá verificar y garantizar que no se violen los requerimientos de seguridad que debe cumplir el software.
- Efectuar las actividades relativas al cambio en el ambiente de desarrollo.
- Las pruebas deben ser realizadas en el ambiente correspondiente y las mismas deben ser aprobadas por parte del usuario final autorizado para tal fin.
- Actualizar la documentación para cada cambio implementado, tanto de los manuales de usuario como de la documentación operativa.
- Mantener un control de versiones para todas las actualizaciones de software.
- Garantizar que la implementación se llevará a cabo minimizando la discontinuidad de las actividades y sin alterar los procesos involucrados.
- Informar a las áreas usuarias antes de la implementación de un cambio que pueda afectar sus operaciones.
- Será el Departamento de Sistemas quien efectúe la actualización de los datos en el nuevo sistema de información.

- Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo

Control: Las aplicaciones críticas para el negocio se deberían revisar y probar para garantizar que no se han generado impactos adversos en las operaciones o en la seguridad de la organización.

Aplicación: Cuando sea necesario realizar un cambio en el sistema operativo, éste debe ser revisado con el fin de verificar que no se genere un impacto negativo en su funcionamiento o seguridad. Para ello se definirá un procedimiento que tenga en cuenta:

- Revisar los procedimientos de integridad y control de aplicaciones para garantizar que no hayan sido comprometidas por el cambio.
- Garantizar que los cambios en el sistema operativo sean informados con anterioridad a la implementación.
- Asegurar la actualización del Plan de Continuidad del Negocio de la Organización.

- Restricciones a los cambios en los paquetes de software

Control: Se deberían evitar modificaciones en los paquetes de software suministrados por terceros, limitándose a cambios realmente necesarios. Todos los cambios se deberían controlar estrictamente.

Aplicación: En caso de requerirse un cambio o modificación en los paquetes de software suministrados por proveedores, previa validación y autorización del Departamento de Sistemas, se deberá:

- Analizar los términos y condiciones de la licencia a fin de determinar si las modificaciones se encuentran autorizadas.
- Determinar la conveniencia de que la modificación sea efectuada por la Organización, por el proveedor o por un tercero.
- Evaluar el impacto que se produce si la Organización se hace cargo del mantenimiento.
- Retener el software original realizando los cambios sobre una copia perfectamente identificada, documentando exhaustivamente por si fuera necesario aplicarlo a nuevas versiones.

- Uso de principios de ingeniería en protección de sistemas

Control: Se deberían establecer, documentar, mantener y aplicar los principios de seguridad en ingeniería de sistemas para cualquier labor de implementación en el sistema de información.

Aplicación: el Área de Sistemas de la Organización aplicará los principios de ingeniería de sistemas, documentando y aplicando procesos seguros en la implementación de cualquier sistema de información.

- Seguridad en entornos de desarrollo

Control: Las organizaciones deberían establecer y proteger adecuadamente los entornos para las labores de desarrollo e integración de sistemas que abarcan todo el ciclo de vida de desarrollo del sistema.

Aplicación: el Área de Sistemas de la organización deberá definir y establecer formalmente la documentación requerida en las diferentes etapas de ciclo de vida de los sistemas.

- Externalización del desarrollo de software

Control: La organización debería supervisar y monitorear las actividades de desarrollo del sistema que se hayan externalizado.

Aplicación: En caso de que la Organización requiera del desarrollo de software por parte de terceros, deberá establecer normas y procedimientos que contemplen lo siguiente:

- Acuerdos de licencias, propiedad de código y derechos conferidos (Derechos de propiedad intelectual (DPI)).
- Requerimientos contractuales con respecto a la calidad del código y la existencia de garantías.
- Procedimientos de certificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, que incluyan auditorías, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad del software establecidos, etc.
- Verificación del cumplimiento de las políticas de seguridad existentes en la Organización (ver objetivo 15.1 SEGURIDAD INFORMÁTICA EN LAS RELACIONES CON SUMINISTRADORES).
- Una vez finalizado el proyecto software, el contratista entregará a la Organización el código fuente, manuales de usuario, documentos de ingeniería de software y cualquier tipo de información relacionada con el mismo.

- Pruebas de funcionalidad durante el desarrollo de los sistemas

Control: Se deberían realizar pruebas de funcionalidad en aspectos de seguridad durante las etapas del desarrollo.

Aplicación: el Área de Sistemas de la Organización deberá llevar a cabo las pruebas de la funcionalidad durante el desarrollo del sistema, las cuales deberán quedar debidamente documentadas.

- Pruebas de aceptación

Control: Se deberían establecer programas de prueba y criterios relacionados para la aceptación de nuevos sistemas de información, actualizaciones y/o nuevas versiones.

Aplicación: El Departamento de Sistemas deberá establecer los requisitos para poner en producción un sistema nuevo o una actualización a un sistema ya existente.

Antes de pasar a ambientes de producción se requiere realizar las pruebas de funcionamiento en ambientes de pruebas, en compañía de los usuarios que utilizarán la aplicación para conocer que todas las formas a actualizar o poner en producción satisfacen las necesidades expuestas por los usuarios, antes definidas en los requisitos funcionales entregados.

Igualmente deberán definir la documentación necesaria para llevar a cabo este procedimiento. (Pruebas de usuario, formatos de actualización de versiones)

12.10.2 DATOS DE PRUEBA

- Protección de los datos utilizados en prueba

Control: Los datos de pruebas se deberían seleccionar cuidadosamente y se deberían proteger y controlar.

Aplicación: Las pruebas de los sistemas se efectuarán sobre datos extraídos del ambiente operativo. Para proteger los datos de prueba se establecerán normas y procedimientos que contemplen lo siguiente:

- Prohibir el uso de bases de datos operativas. En caso contrario se deben despersonalizar los datos antes de su uso. Aplicar idénticos procedimientos de control de acceso que en la base de producción.
- Solicitar autorización formal para realizar una copia de la base operativa como base de prueba, llevando registro de tal autorización.
- Eliminar inmediatamente, una vez completadas las pruebas, la información operativa utilizada.

12.11 RELACIONES CON SUMINISTRADORES

12.11.1 SEGURIDAD INFORMÁTICA EN LAS RELACIONES CON SUMINISTRADORES

- Política de Seguridad Informática para suministradores

Control: Se deberían acordar y documentar adecuadamente los requisitos de Seguridad Informática requeridos por los activos de la organización con el objetivo de mitigar los riesgos asociados al acceso por parte de proveedores y terceras personas.

Aplicación: Cuando exista la necesidad de otorgar acceso a terceras partes a la información de la Organización, el Departamento de Sistemas y el propietario de la información, llevarán a cabo y documentarán una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta, entre otros aspectos:

- El tipo de acceso requerido (físico/lógico y a qué recurso).
- Los motivos para los cuales se solicita el acceso.
- El valor de la información.
- Los controles empleados por la tercera parte.
- La incidencia de este acceso en la Seguridad Informática de la Organización.
- Tener estrategias para evitar el mínimo necesario de permisos a otorgar.

Los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, deben quedar claramente estipulados dentro del contrato de prestación de servicios a firmar entre las partes. Dentro de los acuerdos con terceros, se debe incluir:

- Cumplimiento de la Política de Seguridad Informática de la Organización.

- Protección de los activos de la Organización, incluyendo:
  - Procedimientos para proteger los bienes de la Organización, abarcando los activos físicos, la información y el software.
  - Procedimientos para determinar si ha ocurrido algún evento que comprometa los bienes, por ejemplo, debido a pérdida o modificación de datos.
  - Controles para garantizar la recuperación o destrucción de la información y los activos al finalizar el contrato o acuerdo, o en un momento convenido durante la vigencia del mismo.
  - Restricciones a la copia y divulgación de información.

  - Descripción de los servicios disponibles.
  - Nivel de servicio esperado y niveles de servicio aceptables.

    - Permiso para la transferencia de personal cuando sea necesario.
    - Obligaciones de las partes emanadas del acuerdo y responsabilidades legales.
- Existencia de Derechos de Propiedad Intelectual.
- Definiciones relacionadas con la protección de datos.
- Acuerdos de control de accesos que contemplen:
    - Métodos de acceso permitidos, y el control y uso de identificadores únicos como identificadores de usuario y contraseñas de usuarios.
    - Proceso de autorización de accesos y privilegios de usuarios.
    - Requerimiento para mantener actualizada una lista de individuos autorizados a utilizar los servicios que han de implementarse y sus derechos y privilegios con respecto a dicho uso.

- Definición de criterios de desempeño comprobables, de monitoreo y de presentación de informes.
- Adquisición de derecho a auditar responsabilidades contractuales o surgidas del acuerdo.
- Establecimiento de un proceso para la resolución de problemas y en caso de corresponder disposiciones con relación a situaciones de contingencia.
- Responsabilidades relativas a la instalación y al mantenimiento de hardware y software.
- Estructura de dependencia y del proceso de elaboración y presentación de informes que contemple un acuerdo con respecto a los formatos de los mismos.
- Proceso claro y detallado de administración de cambios.
- Controles de protección física requeridos y los mecanismos que aseguren la implementación de los mismos.
- Métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad.
- Controles que garanticen la protección contra software malicioso.
- Elaboración y presentación de informes, notificación e investigación de incidentes y violaciones relativos a la seguridad.
- Relación entre proveedores y subcontratistas.

- Tratamiento del riesgo dentro de acuerdos de suministradores

Control: Se deberían establecer y acordar todos los requisitos de Seguridad Informática pertinentes a cada proveedor que puede acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI que dan soporte a la información de la organización.

Aplicación: Todos los requisitos de seguridad informática pertinentes serán establecidos y acordados con cada proveedor que pueda acceder, procesar,

almacenar, comunicar, o proporcionar los componentes de infraestructura de TI para la información la Organización, quedando éstos debidamente estipulados en el contrato con el respectivo proveedor.

- Cadena de suministro en tecnologías de la información y comunicaciones

Control: Los acuerdos con los proveedores deberían incluir los requisitos para abordar los riesgos de Seguridad Informática asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones.

Aplicación: la Organización incluirá en el respectivo contrato los requisitos para los acuerdos con proveedores para abordar los riesgos de la seguridad de la información asociada con los servicios de las tecnologías de información y comunicación y de la cadena de suministro de productos.

12.11.2 GESTIÓN DE LA PRESTACIÓN DEL SERVICIO POR SUMINISTRADORES

- Supervisión y revisión de los servicios prestados por terceros

Control: Las organizaciones deberían monitorear, revisar y auditar la presentación de servicios del proveedor regularmente.

Aplicación: Con el fin de garantizar que tanto el acceso a la información, como la prestación de los servicios por parte de terceros se dé bajo las políticas de la Organización, la misma se encargará de realizar auditorías periódicas al tercero, siguiendo los procedimientos establecidos al interior de la entidad para las mismas. Dicho acuerdo debe ser firmado y aceptado por el tercero, bajo las condiciones indicadas por la Organización.

- Gestión de cambios en los servicios prestados por terceros

Control: Se deberían administrar los cambios a la provisión de servicios que realizan los proveedores manteniendo y mejorando: las políticas de Seguridad Informática, los procedimientos y controles específicos. Se debería considerar la criticidad de la información comercial, los sistemas y procesos involucrados en el proceso de reevaluación de riesgos.

Aplicación: Cualquier cambio o modificación en los servicios por terceras partes, deberá estar debidamente sustentado y autorizado por la Organización, siguiendo las políticas internas de la entidad, y teniendo como referencia lo establecido en

los objetivos 12.1.2 Gestión de cambios y 14.2.2 Procedimientos de control de cambios en los sistemas.

12.12 GESTIÓN DE INCIDENTES
12.12.1 GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA Y MEJORAS

- Responsabilidades y procedimientos

Control: Se deberían establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de Seguridad Informática.

Aplicación: La Organización establecerá funciones y procedimientos de manejo de incidentes garantizando una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad (Ver objetivo 16.1.2 Notificación de los eventos de Seguridad Informática). Se deben considerar los siguientes ítems:

- Contemplar y definir todos los tipos probables de incidentes relativos a seguridad, incluyendo:
  - Fallas operativas
  - Código malicioso
  - Intrusiones
  - Fraude informático
  - Error humano
  - Catástrofes naturales

- Comunicar los incidentes a través de canales gerenciales apropiados tan pronto como se tenga conocimiento del incidente, de acuerdo a lo indicado en el objetivo “Comunicación de Incidentes Relativos a la Seguridad”.
-

- Contemplar los siguientes puntos en los procedimientos para los planes de contingencia normales (diseñados para recuperar sistemas y servicios tan pronto como sea posible):
- Definición de las primeras medidas a implementar.
- Análisis e identificación de la causa del incidente.
- Planificación e implementación de soluciones para evitar la repetición del mismo, si fuera necesario.
- Comunicación con las personas afectadas o involucradas con la recuperación, del incidente.
- Notificación de la acción a la autoridad y/u Organismos pertinentes.

- Registrar pistas de auditoría y evidencia similar para:
  - Análisis de problemas internos.
  - Uso como evidencia en relación con una probable violación contractual o infracción normativa, o en marco de un proceso judicial (ver objetivo 18.1 CUMPLIMIENTO DE LOS REQUISITOS LEGALES Y CONTRACTUALES).
  - Negociación de compensaciones por parte de los proveedores de software y de servicios.

- Implementar controles detallados y formalizados de las acciones de recuperación respecto de las violaciones de la seguridad y de corrección de fallas del sistema, garantizando:
  - Acceso a los sistemas y datos existentes sólo al personal claramente identificado y autorizado.
  - Documentación de todas las acciones de emergencia emprendidas en forma detallada.
  - Comunicación de las acciones de emergencia al personal encargado de restablecer el servicio y revisión de su cumplimiento.
  - Constatación de la integridad de los controles y sistemas de la Organización en un plazo mínimo.

En los casos en los que se considere necesario, se solicitará la participación del área jurídica de la organización en el tratamiento de incidentes de seguridad ocurridos y sus implicaciones en todos los niveles.

- Notificación de los eventos de Seguridad Informática

Control: Los eventos de Seguridad Informática se deberían informar lo antes posible utilizando los canales de administración adecuados.

Aplicación: Los incidentes relativos a la seguridad serán comunicados a través de canales gerenciales apropiados tan pronto como se tenga conocimiento del incidente.

Se establecerá un procedimiento formal de comunicación y de respuesta a incidentes, indicando la acción que ha de emprenderse al recibir un informe sobre incidentes.

Dicho procedimiento deberá contemplar que ante la detección de un supuesto incidente o violación de la seguridad, el Departamento de Sistemas sea informado tan pronto como se haya tomado conocimiento. Este indicará los recursos necesarios para la investigación y resolución del incidente, y se encargará de su monitoreo. Así mismo, mantendrá al Comité de Seguridad al tanto de la ocurrencia de incidentes de seguridad.

La Organización evaluará el incidente, y si lo estima pertinente, informará a las autoridades competentes de la ocurrencia del mismo.

La Organización dará a conocer a todos sus funcionarios y personal externo que esté en labores para la misma, el procedimiento de comunicación de incidentes de seguridad, de modo que tan pronto se tenga conocimiento de la ocurrencia de uno, éste sea informado oportunamente.

- Notificación de puntos débiles de la seguridad

Control: Se debería requerir anotar e informar sobre cualquier debilidad sospechosa en la Seguridad Informática en los sistemas o servicios tanto a los empleados como a contratistas que utilizan los sistemas y servicios de información de la organización.

Aplicación: Es responsabilidad de los funcionarios informar de cualquier incidente de seguridad del que tenga conocimiento directo o indirecto, con el fin de tomar las acciones para mitigar los posibles impactos del mismo.

Ningún funcionario está autorizado para realizar pruebas para detectar posibles fallas de seguridad; dichas acciones sólo podrán ser realizadas por el personal designado para tal fin.

- Valoración de eventos de Seguridad Informática y toma de decisiones

Control: Se deberían evaluar los eventos de Seguridad Informática y decidir su clasificación como incidentes.

Aplicación: la Organización evaluará los eventos de Seguridad Informática ocurridos en su interior, a fin de valorarlos y clasificarlos o no como incidentes; lo anterior con el objetivo de realizar la corrección pertinente sobre los hallazgos arrojados en la evaluación de dichos eventos.

- Respuesta a los incidentes de seguridad

Control: Se debería responder ante los incidentes de Seguridad Informática en atención a los procedimientos documentados.

Aplicación: la Organización proporcionará los recursos suficientes para dar una respuesta efectiva de funcionarios y procesos en caso de contingencia o eventos catastróficos que se presenten en la misma y que afecten la continuidad de su operación. Además, responderá de manera efectiva ante eventos catastróficos según la magnitud y el grado de afectación de los mismos; se restablecerán las operaciones con el menor costo y pérdidas posibles, manteniendo la seguridad de

la información durante dichos eventos. La Organización mantendrá canales de comunicación adecuados hacia funcionarios, proveedores y terceras partes interesadas.

- Aprendizaje de los incidentes de Seguridad Informática

Control: Se debería utilizar el conocimiento obtenido del análisis y la resolución de incidentes de Seguridad Informática para reducir la probabilidad y/o impacto de incidentes en el futuro.

Aplicación: La Organización definirá un proceso para documentar, cuantificar y monitorear los tipos, volúmenes y costos de los incidentes y anomalías de seguridad, con el fin de identificar aquellos que sean recurrentes o de mayor impacto para la entidad. Lo anterior, será evaluado a efectos de establecer si es necesario mejorar o agregar nuevos controles para mitigar el impacto de eventos futuros

- Recopilación de evidencias

Control: La organización debería definir y aplicar los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia.

Aplicación: Es necesario contar con adecuada evidencia para respaldar una acción contra una persona u organización. Siempre que esta acción responda a una medida disciplinaria interna, la evidencia necesaria estará descrita en los procedimientos internos.

Cuando la acción implique la aplicación de una ley, tanto civil como penal, la evidencia presentada debe cumplir con lo establecido por las normas procesales.

Para lograr la validez de la evidencia, la Organización garantizará que sus sistemas de información cumplen con la normatividad y los estándares o códigos de práctica relativos a la producción de evidencia válida.

Para lograr la calidad y totalidad de la evidencia es necesaria una sólida pista de la misma. Esta pista se establecerá cumpliendo las siguientes condiciones:

- Almacenar los documentos en papel originales en forma segura y mantener registros acerca de quién lo halló, dónde se halló, cuándo se halló y quién presenció el hallazgo. Cualquier investigación debe garantizar que los originales no sean alterados.

- Copiar la información para garantizar su disponibilidad. Se mantendrá un registro de todas las acciones realizadas durante el proceso de copia. Se almacenará en forma segura una copia de los medios y del registro.

Cuando se detecta un incidente, puede no resultar obvio si éste derivará en una demanda legal por lo tanto se deben tomar todos los recaudos establecidos para la obtención y preservación de la evidencia.

Ante cualquier medida legal que involucre personas ajenas a la Organización u otras organizaciones, la entidad deberá contar con asesoría jurídica a fin de no incurrir en violaciones a la ley y a los derechos sobre quien recaiga la acción judicial.

12.13 ASPECTOS DE LA SI EN LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO
12.13.1 CONTINUIDAD DE LA SEGURIDAD INFORMÁTICA

- Planificación de la continuidad de la Seguridad Informática

Control: La organización debería determinar los requisitos para la Seguridad Informática y su gestión durante situaciones adversas como situaciones de crisis o de desastre.

- Implantación de la continuidad de la Seguridad Informática

Control: La organización debería establecer, documentar, implementar y mantener los procesos, procedimientos y controles para garantizar el mantenimiento del nivel necesario de Seguridad Informática durante situaciones adversas.

- Verificación, revisión y evaluación de la continuidad de la Seguridad Informática

Control: La organización debería verificar regularmente los controles de continuidad de Seguridad Informática establecidos e implementados para poder garantizar su validez y eficacia ante situaciones adversas.

Estos controles están contemplados en el Plan de Continuidad del Negocio de la Organización.

12.13 REDUNDANCIAS

- Disponibilidad de instalaciones para el procesamiento de la información

Control: Se debería implementar la suficiente redundancia en las instalaciones de procesamiento de la información y en correspondencia con los requisitos de disponibilidad.

Aplicación: la Organización propenderá por la existencia de una plataforma tecnológica redundante que satisfaga los requerimientos de disponibilidad aceptables para la misma.

12.14 CUMPLIMIENTO
12.14.1 CUMPLIMIENTO DE LOS REQUISITOS LEGALES Y CONTRACTUALES

- Identificación de la legislación aplicable

Control: Se deberían identificar, documentar y mantener al día de manera explícita para cada sistema de información y para la organización todos los requisitos estatutarios, normativos y contractuales legislativos junto al enfoque de la organización para cumplir con estos requisitos.

Aplicación: La Organización está obligada a cumplir la normatividad vigente que rige para empresas dedicadas al tratado de información sensible de índole personal, la cual se manifiesta en cumplimiento del artículo 10 del Decreto 1377 de 2013 y por medio del cual se reglamenta la Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales” y la ley 1273 de 2009 que creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes. El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “De la Protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”., así como cualquier reglamentación que emane el gobierno nacional y que impacte directamente en el sistema.

- Derechos de propiedad intelectual (DPI)

Control: Se deberían implementar procedimientos adecuados para garantizar el cumplimiento con los requisitos legislativos, normativos y contractuales relacionados con los derechos de propiedad intelectual y utilizar productos de software originales.

Aplicación: Cualquier cambio que afecte los activos software (actualización, instalación, desinstalación), debe ser solicitado por los usuarios al Departamento

de Sistemas, quienes serán los únicos responsables de ejecutar los mismos, una vez evaluada la solicitud y verificada su pertinencia. Estos cambios serán debidamente documentados y sus soportes quedarán en custodia del Departamento de Sistemas. Bajo ninguna circunstancia un cambio puede ser aprobado, realizado e implantado por usuarios diferentes a los responsables del Departamento de Sistemas.

El Departamento de Sistemas efectuará la instalación de software debidamente licenciado, además de que verificará que no se exceda el número máximo permitido de usuarios por cada licencia adquirida. Dichas licencias serán tramitadas por el área de Compras de la Organización.

Los terceros que realicen producciones para la Organización, cederán sus derechos de autor, bajo el entendido que la Organización no podrá realizar ningún tipo de modificación o alteración a dicha producción. Cuando se haga uso de material de un tercero que no se haya cedido a la Organización, ésta deberá efectuar los respectivos créditos.

- Protección de los registros de la organización

Control: Los registros se deberían proteger contra pérdidas, destrucción, falsificación, accesos y publicación no autorizados de acuerdo con los requisitos legislativos, normativos, contractuales y comerciales.

Aplicación: Toda información soportada por la infraestructura de tecnología informática de la Organización deberá ser almacenada y respaldada de acuerdo con las normas emitidas de tal forma que se garantice su disponibilidad.

Debe existir una definición formal de la estrategia de generación, retención y rotación de las copias de seguridad.

La entidad definirá la custodia de los respaldos de la información que se realizará externamente con una compañía especializada en este tema.

El almacenamiento de la información de la entidad deberá realizarse interna y/o externamente, esto de acuerdo con la importancia que dicha información tenga para las operaciones de la Organización.

En cuanto a los soportes de información físicos, la Organización aplicará los controles que tiene establecidos para tal fin, los cuales se ajustan a la normatividad en esa materia, con el fin de garantizar la conservación de dichos soportes y efectuar una debida destrucción de los mismos, cuando sea necesario.

- Protección de datos y privacidad de la información personal

Control: Se debería garantizar la privacidad y la protección de la información personal identificable según requiere la legislación y las normativas pertinentes aplicables que correspondan.

Aplicación: Periódicamente la Organización realizará capacitaciones al personal, en cuanto al manejo y suministro de información, no sólo personal sino también de la que se gestiona día a día en desarrollo de los procesos de la misma, con el fin de generar compromisos frente a la responsabilidad que todos tienen en materia de Seguridad Informática.

Cada funcionario deberá firmar una cláusula de confidencialidad, con la cual se hace responsable del apropiado manejo de la información que genere durante sus labores en la Organización; así mismo, se hará responsable de cualquier daño o perjuicio causado a la empresa derivado del incumplimiento doloso o culposo de dicha obligación.

- Regulación de los controles criptográficos

Control: Se deberían utilizar controles de cifrado de la información en cumplimiento con todos los acuerdos, la legislación y las normativas pertinentes.

Aplicación: Pese a que en Colombia no se encuentra debidamente reglamentado el uso de controles criptográficos, es obligación de la Organización hacer las gestiones y consultas legales pertinentes para el uso de los mismos, a fin de no incurrir en faltas a la ley, ya sea para el manejo de información dentro o fuera del país.

Para el uso de firmas digitales, la Organización deberá ceñirse a lo estipulado en la Ley 527 de 1999, el Decreto 1747 de 2000 y la Circular 10 de la Superintendencia de Industria y Comercio.

12.14.2 REVISIONES DE LA SEGURIDAD INFORMÁTICA

- Revisión independiente de la Seguridad Informática

Control: Se debería revisar el enfoque de la organización para la implementación (los objetivos de control, los controles, las políticas, los procesos y procedimientos para la Seguridad Informática) y gestión de la Seguridad Informática en base a revisiones independientes e intervalos planificados o cuando tengan lugar cambios significativos en la organización.

- Cumplimiento de las políticas y normas de seguridad

Control: Los gerentes deberían revisar regularmente el cumplimiento del procesamiento y los procedimientos de información dentro de su área de responsabilidad respecto a las políticas, normas y cualquier otro tipo de requisito de seguridad correspondiente.

Aplicación: Es responsabilidad del Comité de Dirección realizar una evaluación periódica de los procedimientos definidos para garantizar la Seguridad Informática dentro de la Organización, a fin de evaluar su eficacia y efectividad y tomar las acciones correctivas pertinentes o si es del caso replantear las políticas que no proporcionan los resultados esperados por la Organización.

- Comprobación del cumplimiento

Control: Los sistemas de información se deberían revisar regularmente para verificar su cumplimiento con las políticas y normas de seguridad dispuestas por la información de la organización.

Aplicación: El Departamento de Sistemas verificará periódicamente que los sistemas de información cumplan con la política, normas y procedimientos de seguridad, las que incluirán la revisión de los sistemas en producción a fin de garantizar que los controles de hardware y software hayan sido correctamente implementados. En caso de ser necesario, estas revisiones contemplarán la asistencia técnica especializada.

El resultado de la evaluación debe quedar consignado en un informe técnico para su interpretación por parte de los especialistas. Para ello, la tarea podrá ser realizada por un profesional experimentado (en forma manual o con el apoyo de herramientas de software), o por un paquete de software automatizado que genere reportes que serán interpretados por un especialista técnico.

La verificación del cumplimiento comprenderá pruebas de penetración y tendrá como objetivo la detección de vulnerabilidades en el sistema y la verificación de la eficacia de los controles con relación a la prevención de accesos no autorizados. Se tomarán los recaudos necesarios en el caso de pruebas de penetración exitosas que comprometan la seguridad del sistema.

Las verificaciones de cumplimiento sólo serán realizadas por personas competentes, formalmente autorizadas y bajo la supervisión.

13. PLAN DE CONTINUIDAD DEL NEGOCIO PARA LA EMPRESA CONFECAMARAS

13.1 ANTECEDENTES

En marco a lo establecido en el numeral 17. ASPECTOS DE LA SI EN LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO del Anexo A de la NTC ISO 27001:2013, a continuación se desarrollará un Plan de Continuidad del Negocio para CONFECAMARAS.

Una vez surtido el proceso de Análisis y Gestión de Riesgos donde se identificaron los procesos, las aplicaciones, el hardware y otros activos críticos de la organización, además de los usuarios involucrados con éstos, se determinó lo siguiente:

13.2 CONSIDERACIÓN DEL PERIODO MÁXIMO DE INTERRUPCIÓN

Dadas las condiciones del negocio y de los procesos asociados a él, como primera instancia definiremos el costo diario de las operaciones de los procesos en estudio, con el fin de tener una visión financiera de las pérdidas ocasionadas ante un posible incidente grave; dentro de estos costos no se tienen en cuenta aspectos no cuantificables como la imagen de la organización, dado que éste tipo de intangibles son de difícil traducción a cifras monetarias. Lo que sí es claro, es que la organización goza de una muy buena reputación ante la comunidad en general, y cualquier evento que impacte de forma negativa sobre su nombre, genera una visión igualmente negativa en la población.

Para este caso puntual se tuvo en cuenta el costo de los procesos (Tabla 12), y los mismos se discriminan de la siguiente forma:

Tabla 12: Costos por procesos en Confecámaras

COSTOS POR PROCESOS EN CONFECAMARAS.		
ITEM	**VALOR PROMEDIO MENSUAL PESOS**	**VALOR PROMEDIO DIARIO PESOS**
Desarrollo de aplicaciones	44.770.593	1.492.353
Afinamiento de aplicaciones	93.771.200	3.125.707
Mantenimiento de aplicaciones	710.250.000	23.675.000
Prueba de aplicaciones	208.080.600	6.936.020
Gestión operativa y administrativa	2.074.250.000	69.141.667
Totales	**$ 3.131.122.393**	**$ 104.370.746**

Teniendo en cuenta lo anterior, lo ideal para la organización es que el paro en sus procesos sea máximo de 4 horas, en razón al impacto financiero antes descrito.

De igual forma, y aun cuando se tenga un Plan de Continuidad del Negocio debidamente validado, existen incidentes graves que podrían afectar seriamente la eficacia y efectividad de dicho plan, ya que no sólo se ven afectadas las operaciones de la organización Confecámaras puntualmente, sino también las operaciones de sus aliadas naturales, las Cámaras de Comercio, con convenio tecnológico adscrito, en primer plano, y en segundo plano todas las demás por los servicio centralizados que ofrece la Confederación.

13.3 ESTRATEGIA DE RESPALDO

“En esta fase se identificarán los métodos operativos alternativos que se tendrán a disposición en el momento en que una amenaza se materialice o de que ocurra un incidente que provoque una interrupción en la organización.

El método dispuesto deberá ofrecer amplias garantías sobre la restauración de los procesos afectados en los tiempos determinados por el análisis de Impacto.”

13.4 SELECCIÓN DE ESTRATEGIAS

Teniendo en cuenta los procesos objeto de estudio y la infraestructura con la que la organización cuenta, la siguiente, es la estrategia prevista en el evento de que ocurra una situación que impacte directamente sobre dichos procesos, generando traumatismos en su desarrollo:

- Instalaciones físicas: La organización cuenta con la sede denominada "Unidad de Servicios DRP Synapsis" en la zona franca de Fontibón, dotada con amplias salas de sistemas, salones, escritorios, los cuales funcionarían como puestos de trabajo, en caso de ser requerido. Sumado a ello, dicha sede se encuentra en las afueras de la ciudad, lo que no implicaría traumatismos al momento de que los usuarios necesiten acceder a los servicios con una infraestructura espejo con la topología semejante a la de la sede principal tipo cloud.

- Hardware: cómo se mencionó anteriormente, dicha sede cuenta con equipos de cómputo con las características necesarias para funcionar, atendiendo a las necesidades de los procesos de la Organización, en su capacidad total operativa.

Frente a los servidores y otros equipos de almacenamiento y procesamiento de información adicionales, se tiene pactado un contrato con la empresa de hardware INTELLIGENT SOLUTIONS COMPANY radicada en la ciudad de Bogotá y proveedor de servicios varios de consultoría a la entidad para cloud computing. En dicho contrato se establece proporcionar en calidad de alquiler, los equipos requeridos con las especificaciones dadas por la organización, para minimizar el tiempo de interrupción de los procesos antes mencionados, no obstante la sala "Unidad de Servicios DRP Synapsis" proporciona equipo de mediana capacidad de cómputo para el uso de los usuarios Tipo1. ISC sería la encargada de proporcionar los equipos de cómputo de mayor capacidad, servidores y almacenamiento.

- Software: dado que el software requerido para el desarrollo de los procesos de Programación y Operatividad administrativa es producido por la organización, ésta debe contar con una copia de los mismos, debidamente almacenada en un servidor tipo "cloud", en caso de que ocurra un siniestro y los servidores y equipos donde opera, queden fuera de servicio.

- Soportes de información: la Organización cuenta con un procedimiento debidamente documentado para el manejo de las copias de seguridad de la información contenida en los equipos de almacenamiento de la organización, de igual manera cuenta con un procedimiento de archivo debidamente implementado,

el cual permite tener digitalmente todos y cada uno de los soportes de información (como formularios, cartas, actas, comprobantes de pago) los cuales son importantes para el desarrollo de los procesos objeto de trabajo.

- Redes de comunicación y servicios: La Unidad de Servicios DRP Synapsis, cuenta con una red de comunicaciones capaz de soportar el flujo de comunicaciones y de datos de los procesos en estudio, de igual manera cuenta con servicio de internet ilimitado.

- Personas: con el fin de minimizar al máximo la interrupción de los procesos en lo que respecta al personal, se procederá a capacitar a cada uno de los funcionarios de las áreas dueñas de los procesos en estudio, con el fin de que cada uno conozca y desarrolle sin limitantes los puestos de trabajo o subprocesos propios de cada una, con el fin de que si algún funcionario esté ausente, otro esté en las condiciones cognitivas para reemplazarlo, sin que el subproceso se vea seriamente afectado y minimizando al máximo los tiempos de interrupción del mismo.

A futuro puede proyectarse la adecuación de un centro de datos en la Unidad de Servicios, con las mismas características del centro de datos de la sede principal, lo que se conoce como un “Centro Espejo”, con el fin de que las estrategias para restaurar el servicio impliquen la movilización de personal y adecuaciones menores en cuanto a puestos de trabajo y red de comunicaciones y servicios.

Éste es un proyecto que se planeó cuidadosamente, pues los costos en los que incurriría la organización son altos, viéndolo más que como un gasto, como una inversión.

Como alternativa adicional y en caso de afectaciones extremas, se han implementador opciones de teletrabajo y de trabajo remoto en empresas del sector que ofrecen en sus Datacenters opciones de conectividad. Esto daría un amplio cubrimiento y alternativa de primera mano a cualquier eventualidad, siniestro o catástrofe localizada en la sede principal con repercusión de la sede alterna.

13.4 DESARROLLO DEL PLAN DE CONTINUIDAD

13.4.1 ORGANIZACIÓN DE LOS EQUIPOS

13.4.2 EQUIPO DIRECTOR O COMITÉ DE CRISIS

“El objetivo de este comité es reducir al máximo el riesgo y la incertidumbre en la dirección de la situación. Este Comité debe tomar las decisiones “clave” durante los incidentes, además de hacer de enlace con la dirección de la compañía, manteniéndoles informados de la situación regularmente.

Las principales tareas y responsabilidades de este comité son:

• Análisis de la situación.
• Decisión de activar o no el Plan de Continuidad.
• Iniciar el proceso de notificación a los empleados a través de los diferentes responsables.
• Seguimiento del proceso de recuperación, con relación a los tiempos estimados de recuperación." [1]

Atendiendo a la anterior definición y teniendo en cuenta que dentro del desarrollo de la fase de planeación de la metodología de análisis y gestión de riesgos MAGERIT, se definió un comité de dirección, el cual está integrado por todas aquellas áreas que tienen que ver con los procesos objeto de estudio, desde el punto de vista financiero, de recursos humanos, legal, directivo y obviamente por las personas dueñas de dichos procesos, teniendo en cuenta lo anterior, el comité de crisis es el siguiente, tomando como referente la metodología para análisis y gestión de riesgos MAGERIT, de acuerdo a los cargos más relevantes del organigrama institucional de Confecámaras:

- Presidente Ejecutivo (Dirección de comunicaciones)
- Vicepresidencia Ejecutiva (Web master, Coordinación de compras)
- Director de Operaciones
- Gerencia de cooperación y Colaboración
- Coordinación de Representación
- Gerencia de Servicios Camerales (Jefe de Sistemas, Coordinador de infraestructura)
- Asesoría Administrativa de Control
- Soporte y Servicio al Cliente (Coordinación de soporte y Coordinación de Infraestructura)
- Registro Único Empresarial (RUES) (Área de Desarrollo)

13.4.3 EQUIPO DE RECUPERACIÓN

"El equipo de recuperación es responsable de establecer la infraestructura necesaria para la recuperación. Esto incluye todos los servidores, PC's, comunicaciones de voz y datos y cualquier otro elemento necesario para la restauración de un servicio." [2]
Atendiendo a la anterior definición el equipo de recuperación estaría conformado por las siguientes personas:

- Gerencia de Servicios Camerales
- Jefe de sistemas

[1]Del Pino Jiménez, 2007
[2]Del Pino Jiménez, 2007

- Jefe de desarrollo
- Coordinador de infraestructura
- Webmaster

13.4.4 EQUIPO LOGÍSTICO

"Este equipo es responsable de todo lo relacionado con las necesidades logísticas en el marco de la recuperación, tales como:

- Transporte de material y personas (si es necesario) al lugar de recuperación.
- Suministros de oficina.
- Comida.
- Reservas de hotel, si son necesarias.
- Contacto con los proveedores.

Este equipo debe trabajar conjuntamente con los demás, para asegurar que todas las necesidades logísticas sean cubiertas." [3]

Atendiendo a lo anterior, el equipo logístico estaría conformado por:

- Vicepresidencia ejecutiva
- Coordinador de Compras
- Secretaria División Administrativa

13.4.5 EQUIPO DE RELACIONES PÚBLICAS Y ATENCIÓN A CLIENTES

"Se trata de canalizar la información que se realiza al exterior en un solo punto para que los datos sean referidos desde una sola fuente. Sus funciones principales son:

- Elaboración de comunicados para la prensa.
- Comunicación con los clientes.

Uno de los valores más importantes de una compañía son sus clientes, por lo que es importante mantener informados a los mismos, estableciendo canales de comunicación."[4]

[3]Del Pino Jiménez, 2007
[4]Del Pino Jiménez, 2007

Atendiendo a lo anterior, el equipo de relaciones públicas y atención a clientes estaría conformado por:

- Gerencia de servicios camerales
- Jefe de Comunicaciones

13.4.5 EQUIPO DE LAS UNIDADES DE NEGOCIO

“Estos equipos estarán formados por las personas que trabajan con las aplicaciones críticas, y serán los encargados de realizar las pruebas de funcionamiento para verificar la operatividad de los sistemas y comenzar a funcionar.

Cada equipo deberá configurar las diferentes pruebas que deberán realizar para los sistemas.”

Es importante resaltar que todas las gestiones desarrolladas, durante y después del reporte de un incidente de gran magnitud, serán apoyadas por la Brigada de Emergencia ya establecido al interior de la organización.

13.5 DESARROLLO DE PROCEDIMIENTOS

Es importante resaltar que el diseño de un Plan de continuidad del Negocio, se realiza con el fin de atender y resolver incidentes que involucren la capacidad de operación de la organización o procesos de la misma, en todo lo que a esa operación se refiere: instalaciones físicas, personal, hardware, software, redes de comunicación. Para incidentes menores, la organización tiene implementados controles que le permiten resolver esos incidentes.

13.6 FASE DE ALERTA

“La Fase de Alerta define los procedimientos de actuación ante las primeras etapas de un suceso que implique la pérdida parcial o total de uno o varios servicios críticos.”[5]

13.7 PROCEDIMIENTO PARA LA NOTIFICACIÓN DEL DESASTRE

Cualquier funcionario de la organización que sea consciente de un incidente grave, deberá notificarlo a la Jefatura de Gestión Humana y calidad, como cabeza principal de la Brigada de Emergencia, quien se encargará de informar al Comité

[5]Del Pino Jiménez, 2007

de Crisis, en cabeza del Vicepresidente Ejecutivo, el incidente, con quien analizará la situación problema; se convocará al Comité de Crisis en pleno, para analizar más a fondo el incidente.

13.8 PROCEDIMIENTO DE EJECUCIÓN DEL PLAN

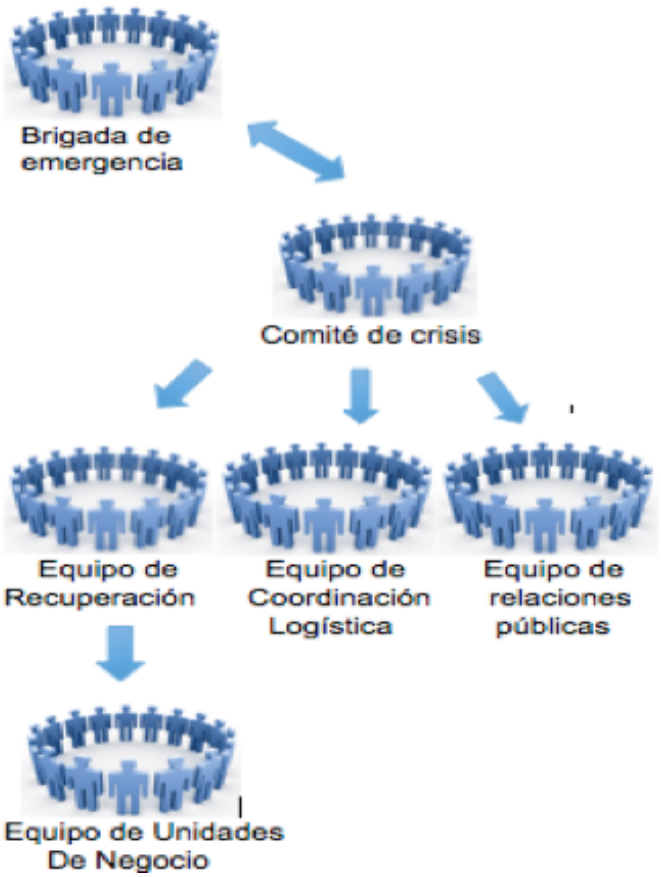
Una vez reunido el Comité de Crisis para evaluar la gravedad del incidente, definirá si se pone en marcha o no el Plan de Continuidad del Negocio:

- De ser afirmativo, se iniciará con la ejecución del plan.
- De ser negativo, dadas las condiciones del incidente y según análisis hecho por el Comité de Crisis, se ejecutarán los controles pertinentes definidos por el comité, para normalizar la situación.

13.9 PROCEDIMIENTO PARA LA EJECUCIÓN DEL PLAN

Activación del árbol de llamadas, conformado por los diferentes equipos que participan en el Plan de Continuidad del Negocio en donde el orden jerárquico, la comunicación efectiva y el seguimiento del protocolo se hacen evidentemente necesarios. El orden inicia con la Brigada de emergencia, quien estará comunicando el estado de la situación al Comité de crisis, el cual a su vez coordinará a los equipos de: Recuperación, coordinación logística, relaciones públicas y equipo de unidades de negocio, el cual está a disposición del equipo de recuperación, y la comunicación podrá será unidireccional o bidireccional, tal como se ilustra en los sentidos de la flecha de la gráfica 7:

Gráfica 7: Árbol de llamadas PCN



Fuente: El autor

13.9 FASE DE TRANSICIÓN

13.9.1PROCEDIMIENTO DE CONCENTRACIÓN Y TRASLADO DE MATERIAL

Una vez surtido el proceso de notificación a todos los equipos del plan, el equipo logístico se encargará de disponer lo necesario para el traslado de personas, equipos y todos los materiales necesarios para la puesta en marcha de las operaciones en la sede alterna designada para tal fin: Unidad de Servicios DRP Synapsis.

13.9.2 PROCEDIMIENTO DE PUESTA EN MARCHA DEL CENTRO DE RECUPERACIÓN

Una vez estén ubicadas en la Unidad de Servicios todas las personas, equipos y materiales necesarios para la puesta en marcha de las operaciones, el equipo de

recuperación se encargará de todas las gestiones pertinentes para tal fin; el equipo logístico hará el acompañamiento al equipo de recuperación, con el fin de atender cualquier requerimiento adicional de insumos necesario para el proceso de recuperación.

13.10 FASE DE RECUPERACIÓN

13.10.1 PROCEDIMIENTO DE RESTAURACIÓN

Conforme a la dependencia entre un proceso y otro, lo primero que se hará es la restauración del Proceso de Sistemas y una vez esté en pleno funcionamiento, se procederá a restaurar los procesos del área operativa y administrativa.

Como primera instancia se procederá a revisar el local donde se adecuarán los centros de trabajo, verificando condiciones físicas, disponibilidad de conexiones para la red de comunicaciones y datos. De ser necesario se procederá con la instalación de las conexiones requeridas para la adecuación de los centros de trabajo.

Una vez listo el local, se procederá con las adecuaciones de muebles de oficina, posteriormente equipos de almacenamiento y de cómputo, teléfonos y cualquier otro tipo de equipamiento físico requerido.

Posteriormente se hará la instalación de software base y software propio de los procesos, se subirán las copias de la información a los servidores; después, se iniciarán las pruebas de conectividad y de comunicación, con el fin que verificar si existe flujo de datos entre los equipos, para los casos en los que los sistemas espejo no alcancen su sincronización optima en cualquiera de los nodos de restauración virtual o física.

Verificado lo anterior, se procederá de la misma manera con los Procesos de administrativos y gerenciales y pasando luego a las áreas de producción, instalando hardware, software y realizando las pruebas necesarias, evidenciando el flujo de datos.

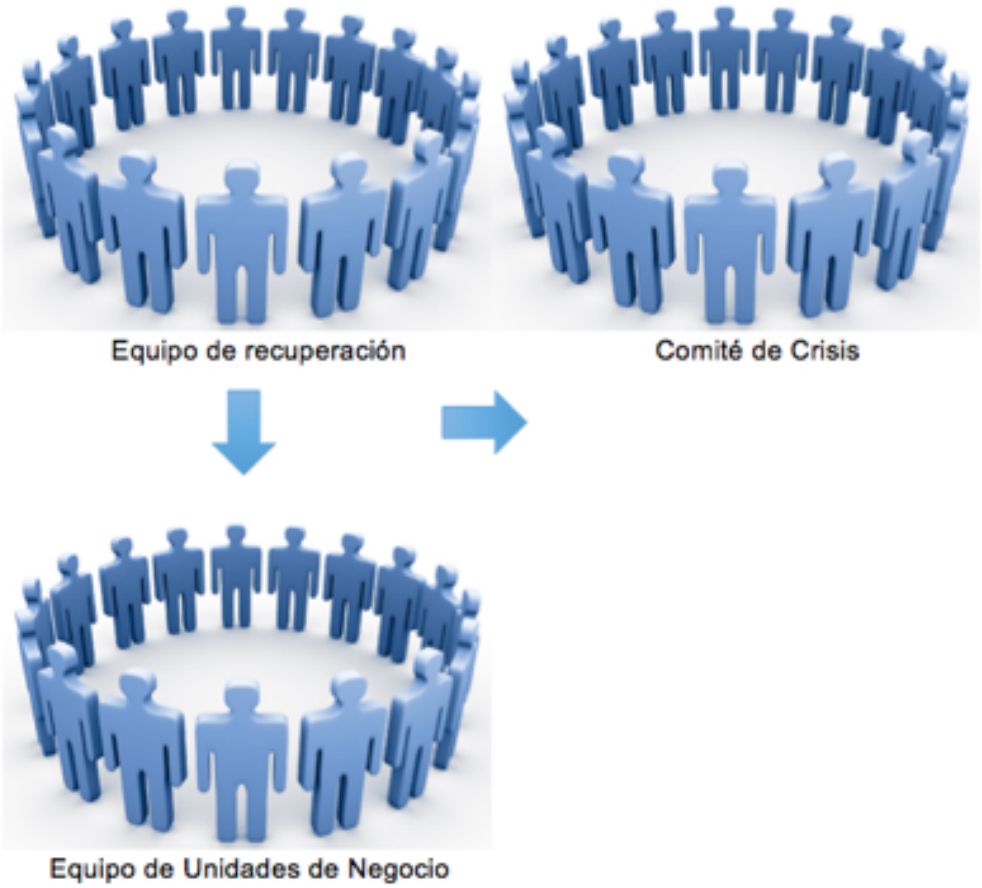
13.11 PROCEDIMIENTO DE SOPORTE Y GESTIÓN

Una vez recuperados los sistemas, se dará aviso a los equipos de unidades de negocio, con el fin de realizar las pruebas pertinentes al software para garantizar la prestación apropiada de los servicios.

Es importante que, dado que el Comité de Recuperación está conformado por el personal profesional y técnico del área de Servicios Camerales, garanticen que la puesta en marcha de las operaciones se hará de manera segura, es decir, en

términos de integridad, confidencialidad y disponibilidad de la información, antes de dar por finalizada la etapa de recuperación suministrando las instrucciones del procedimiento de soporte y gestión en un orden jerárquico preestablecido, como se ilustra en la gráfica 8, en donde el flujo de la información circula en un único sentido, partiendo desde el equipo de recuperación hacia los equipos de comité de crisis y equipo de unidades de negocio, de la siguiente manera:

Gráfica 8: Orden del procedimiento de Soporte y Gestión



Fuente: El autor

13.11 FASE DE VUELTA A LA NORMALIDAD / FIN DE LA EMERGENCIA

13.11.1 ANÁLISIS DE IMPACTO

Para realizar el análisis de impacto, será el Comité de Crisis en pleno, quien designará los equipos o personas encargados de hacer las estimaciones en cuanto a:

- Recursos no reutilizables por la gravedad de los daños causados por el incidente.
- Recursos medianamente afectados, con coste de recuperación.
- Recursos no afectados.
- Costos de mano de obra para recuperar tanto equipos como instalaciones físicas y demás recursos afectados por el incidente.

De igual manera es importante tener claros los costos de las pérdidas ocasionadas por el incidente, no sólo en cuanto a recursos físicos perdidos, sino también en cuanto a servicios dejados de prestar, recursos financieros dejados de percibir, coste de personal inoperante por el evento, entre otros.

13.11.2 ADQUISICIÓN DE NUEVO MATERIAL

Una vez realizada la evaluación de impacto, se determinará la necesidad de adquirir nuevos recursos. Para tal fin, será el Comité de Crisis quien haga los contactos pertinentes con las aseguradoras, con el fin de hacer los trámites respectivos para el reconocimiento de seguros; de igual manera, el Equipo Logístico se encargará de hacer los contactos y gestiones necesarias para la adquisición de nuevos recursos, equipos y material, para reponer las pérdidas ocasionadas por el incidente.

13.12 FIN DE LA CONTINGENCIA

Puede variar entre días, semanas y/o meses, de acuerdo a la gravedad de los daños y a la agilidad en la recuperación y restauración de locales, equipos y demás recursos perdidos a causa del evento.

Lo más importante es que los procesos, clientes y personal de la empresa se vean lo menos afectados por la situación.

Una vez recuperadas completamente las instalaciones objeto del incidente, en el entendido que la recuperación abarca equipamiento físico, hardware, software, muebles de oficina, redes de comunicación y datos, se procederá con el traslado del personal; a su vez, el equipo de comunicaciones se encargará de notificar al público en general de la reanudación de las operaciones en la sede principal.

13.13 GENERACIÓN DE INFORMES Y EVALUACIÓN

Cada equipo de trabajo deberá elaborar un informe de las actividades de trabajo desarrolladas durante y después del incidente, hasta el momento de normalizar las operaciones, con el fin de tener herramientas de evaluación del Plan de Continuidad del Negocio, que le permitan a la organización conocer si el dicho

plan es eficaz y efectivo o si por el contrario requiere ajustes para su óptima operación, cuando la situación así lo demande.

13.14 PRUEBAS Y MANTENIMIENTO
13.14.1 PRUEBAS
13.14.2 OBJETIVOS DEL PLAN DE PRUEBAS

“El Plan de Continuidad no se considerará válido hasta que no se haya superado satisfactoriamente el Plan de Pruebas que asegure la viabilidad de las soluciones adoptadas.

El Plan de Pruebas diseñado tiene como objetivos:

Evaluar la capacidad de respuesta ante una situación de desastre que afecte a los recursos de la compañía.

Probar la efectividad y los tiempos de respuesta del Plan para comprobar que están alineados con la definición realizada en el diseño.

Identificar las áreas de mejora en el diseño y ejecución del Plan.

Comprobar si los procedimientos desarrollados son adecuados para soportar la recuperación de las operaciones de negocio.

Evaluar si los participantes del ejercicio están suficientemente familiarizados con la operativa en situación de contingencia.

Concienciación y formación para los empleados a través de la realización de pruebas.”

13.14.3 TIPOS DE PRUEBAS

“Las pruebas de un Plan de Continuidad deben tener dos características principales:

Realismo: La utilidad de las pruebas se reduce con la selección de escenarios irreales. Por ello es importante reproducir escenarios que proporcionen un nivel de entrenamiento adecuado a las situaciones de riesgo.

Exposición Mínima: Las pruebas deben diseñarse de forma que impacten lo menos posible en el negocio, es decir, que si se programa una prueba que suponga una parada de los sistemas de información, debe realizarse una ventana de tiempo que impacte lo menos posible para el negocio.

En algunos casos puede resultar complicado realizar una prueba completa del Plan de Continuidad de Negocio. Por ello, es necesario desarrollar un programa de pruebas planificado para garantizar que todos los aspectos de los planes y personal se han ensayado durante un período de tiempo." [6]

13.14.4 EJERCICIOS TÉCNICOS

"Este tipo de ejercicio requerirá la ejecución de procedimientos de notificación y operativos, el uso de equipos de hardware, software y posibles centros y métodos alternativos para asegurar un rendimiento adecuado. Ejemplos de elementos verificados durante un ejercicio de simulación son:

Procedimientos de emergencia.
Métodos alternativos.
Líneas de telecomunicaciones de backup.
Procedimientos de notificación Vendedores / Clientes.
Capacidad y rendimiento del hardware.
Portabilidad del software.
Accesibilidad al centro de respaldo.
Movilización de los equipos de trabajo.
Recuperación de ficheros y documentación almacenados en lugar externo.
Recuperación de datos." [7]

13.14.5 TEST COMPLETO

"Los ejercicios de test son ejercicios planificados que implican la restauración real de la capacidad de proceso en un centro alternativo. Generalmente, los procesos en producción no son interrumpidos, pero puede planificarse su restauración y validación en el centro alternativo. Normalmente, este tipo de prueba requiere la participación de toda la organización de continuidad del negocio, incluyendo usuarios, personal técnico y de operaciones."

13.14.6 MANTENIMIENTO DEL PLAN DE CONTINUIDAD

"Por la propia dinámica de negocio, se van incorporando nuevas soluciones a los Sistemas de Información y los activos informáticos van evolucionando para dar respuesta a las necesidades planteadas.

La correcta planificación del mantenimiento del Plan de Continuidad evitará que quede en poco tiempo obsoleto y que en caso de contingencia no pueda dar respuesta a las necesidades." [8]

---

[6]Del Pino Jiménez, 2007
[7]Del Pino Jiménez, 2007

Como se mencionó anteriormente, las pruebas se constituyen en un importante elemento de evaluación al Plan de Continuidad del Negocio, en razón a que simular un incidente nos da las herramientas necesarias para calificar la capacidad de reacción y de operación de los equipos que conforman el plan y de ésta manera realizar los ajustes y cambios pertinentes. Lo ideal de las pruebas es que se hagan con el mayor realismo posible, sin embargo, dados los costos en que la organización deberá incurrir para realizar una prueba "real", deberá incluir dentro de su presupuesto un rubro para tal fin; de igual manera deberá preparar a los funcionarios frente a la realización de la prueba, la cual, para interrumpir en lo menor posible las operaciones y prestación del servicio a los clientes, se realizará en días no hábiles (sábados, domingos y festivos), conforme a cronograma definido por la misma organización.

De igual forma, los controles establecidos por la organización para prever cualquier incidente menor, como la caída del sistema, el deterioro de un equipo de almacenamiento propiciando la pérdida parcial de información, deberán revisarse periódicamente, con el fin de actualizarlos y ajustarlos a la organización y la dinámica de sus procesos, minimizando en gran parte cualquier novedad en las operaciones de la entidad.

No importa que tan grande o pequeña sea una empresa, un Plan de Continuidad del Negocio es una herramienta que le permitirá a cualquier organización no desaparecer por causa de un incidente natural, industrial o de orden público.

14. CRONOGRAMA

El siguiente cronograma fue el propuesto desde la etapa de anteproyecto y en el mismo se sintetizó el avance de las etapas surtidas durante la gestión de análisis del Sistema de Gestión de Seguridad Informática para Confecámaras:

[8]Del Pino Jiménez, 2007

Gráfica9: Cronograma propuesto para el SGSI

CRONOGRAMA PARA LA IMPLEMENTACION UN SISTEMA DE GESTION DE SEGURIDAD INFORMATICA CONFEDERACIÓN COLOMBIANA DE CÁMARAS DE COMERCIO

EVENTO	RESPONSABLE	NIVELES	2015 SEMANAS 1	2	3	4	5
Creación del documento de política de seguridad	Coordinador infraestructura, jefe servicios tecnológicos, gerente servicios camerales	Táctico, estratégico, directivo					
Análisis de requisitos: Requisitos de seguridad de la información para el proceso SGSI	Coordinador infraestructura, jefe servicios tecnológicos	Táctico, estratégico					
Identificar los activos dentro de los limites de alcance del SGSI	Coordinador infraestructura, jefe servicios tecnológicos	Táctico, estratégico					
Evaluación de seguridad de la organización.	Coordinador infraestructura, jefe servicios tecnológicos	Táctico					
Alcance: Declaración de aplicabilidad	Coordinador infraestructura, jefe servicios tecnológicos	Táctico					
Aplicabilidad y Alcance de cubrimiento para el proyecto de implementación biométrica	Coordinador infraestructura, jefe servicios tecnológicos	Táctico					

EVENTO	RESPONSABLE	NIVELES	2015 SEMANAS 1	2	3	4	5
Riesgos: Controles, análisis de vulnerabilidades	Coordinador infraestructura, jefe servicios tecnológicos	Táctico, estratégico					
Analisis diferencial	Coordinador de infraestructura	Táctico					
Revisiones por la Dirección	Coordinador infraestructura, jefe servicios tecnologicos	Táctico, estrategico					
Metricas y auditorias: Internas y externas	Coordinador infraestructura, jefe servicios tecnologicos	Táctico, estrategico					
Documentacion de los procesos	Coordinador infraestructura, jefe servicios tecnologicos, gerente servicios camerales	Táctico, estrategico					
Procedimientos revisión por dirección	Gerente servicios tecnologicos	Directivo					
Procedimientos auditorias internas	Jefe servicios tecnlógicos	Táctico					
Seguimiento, supervision y revision del SGSI	Coordinador infraestructura, jefe servicios tecnologicos, gerente servicios camerales	Táctico, estrategico					
Mantener y mejorar el sistema	Coordinador infraestructura, jefe servicios tecnologicos, gerente servicios camerales	Táctico, estrategico, directivo					
Plan de tratamiento de riesgos	Coordinador infraestructura, jefe servicios tecnologicos	Táctico, estrategico					

EVENTO	RESPONSABLE	NIVELES	2015				
			SEMANAS				
			1	2	3	4	5
Formación, concientización personal	Empleados, contratistas, proveedores de servicios con acceso a recursos operativos.	Tecnico y operativo					

15. CONCLUSIONES

La Implementación y ejecución, bajo la norma ISO 27001:2013 de un Sistema de Gestión de Seguridad de la Información, ha generado un ambiente de seguridad y confianza en los procesos informáticos de la Confederación de Cámaras de Comercio de Colombia - Confecámaras, sin precedentes, en ninguno de sus 45 años de operación.

Tanto por parte de sus usuarios internos como de sus usuarios externos, el plan de seguridad general que la Confederación Colombiana que inicio desde el año 2014 bajo la dirección del área de Servicios Tecnológicos, ha llevado a propiciar en sus clientes confederados, la necesidad de alinear sus operaciones bajo esquemas de seguridad mucho más adaptados a las necesidades de la operación registral en Colombia y ello ha iniciado una nueva cultura de seguridad de la información en las Cámaras de Comercio de Colombia.

Por parte de los usuarios internos, el proceso que se inició a manera de encuestas y definiendo los procesos y activos en las diferentes áreas de Confecámaras, obligo a que todos aquellos servicios y metodologías de trabajo que no se encontraban acordes a prácticas seguras en el manejo de la información, fuesen revalorados y se ajustaran a las nuevas necesidades de seguridad.

El método de análisis y gestión de riesgos estructurado Magerit, permitió evidenciar el estado actual de fallas en los procesos que se ejecutaban a diario dentro de la organización y esto redundo en un incremento en el nivel de seguridad de la información de la entidad creando las bases para la implementación de las políticas de seguridad, la declaración de aplicabilidad y procedimiento de continuidad del negocio dejaran de ser solo una visión futura del debes ser y pasaran a ser el nuevo esquema de seguridad en la información en la Confederación de Cámaras de Comercio.

16. RECOMENDACIONES

Todo sistema que pretenda ser mejorado y sobre todo, cada sistema que pretenda evolucionar, debe someterse a una exhaustiva radiografía de todas sus partes. Se hace necesario entonces pensar en que todo lo que se mide es susceptible de mejora y más aún cuando es la seguridad de la información la que está en juego.

Nunca se puede dar por atendida o por mitigada totalmente una amenaza y mucho menos pensar que el riesgo es algo que se puede asumir y vivir con dicha incertidumbre.

Aún más, cuando pensamos que defendernos de un ataque es solo cuestión de invertir en equipos, se debe dejar por establecido como norma de convivencia con los sistemas de información, que es mucho más fácil atacar un sistema que defenderlo, ninguna guerra se ha ganado sin estrategia.

Vuélvete más silencioso, así estarás en mejor capacidad de escuchar.[9]

[9]Kali Linux Colaborators, 2014

17. BIBLIOGRAFÍA

Ojeda-Pérez, Jorge Eliécer; Rincón-Rodríguez, Fernando; Arias-Flórez, Miguel Eugenio & Daza-Martínez, Libardo Alberto (2010). Delitos informáticos y entorno jurídico vigente en Colombia. Cuadernos de Contabilidad, 11 (28), 41-66.

AVELLA PINZON, Rocío del Pilar; GIL GAMBOA, Manuel Salvador; BOHADA, Jhon A. Realidades de un Delito Informático en Boyacá. Ciencia, Innovación y Tecnología, 2014, vol. 1, p. 83-95.

AGREDO SARRIA, Virginia "ABC PARA PROTEGER LOS DATOS PERSONALES LEY 1581 DE 2012 DECRETO 1377 DE 2013". {En línea}. {10 julio de 2013} disponible en: http://colombiadigital.net/publicaciones_ccd/anexos/certicamara_proteccion_datos_ago28.pdf, Tecnología, 2014, vol. 1, p. 83-95.

CERTICAMARAS "ABC PARA PROTEGER LOS DATOS PERSONALES LEY 1581 DE 2012 DECRETO 1377 DE 2013 – NUEVA EDICIÓN". {En línea}. {15 Mayo de 2014} disponible en: https://web.certicamara.com/media/132739/cartilla-abc-proteccion-de-datos.pdf

ESCOBAR PEÑALVER, Andrés Felipe; PAJARITO CONTRERAS, Mónica Paola. Alcance e implicaciones del derecho al Habeas Data en el comercio colombiano. 2014.

Gaspar del Pino, Juan Jimenéz. Planes de Contingencia la Continuidad del Negocio en las Organizaciones. Ediciones Díaz de Santos, 2007.

Organización internacional de estándares- ISO. Sistema de Gestión de la Seguridad de la Información. Portal ISO 27001 en español. Recuperado de http://www.iso27000.es/sgsi.html
International OrganizationforStandardization, ISO, International ElectrotechnicalCommission, IEC (2005). ISO/IEC 17799/2005. Disponible en: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39612.

TABARES, Claudia María, PINEDA, Juan David "METODOLOGÍA PARA ENTENDER INCIDENTES DE SEGURIDAD INFORMÁTICA EN LA MEDIANA EMPRESA COLOMBIANA". {En línea}. {15 Diciembre de 2007} disponible en: https://publicaciones.eafit.edu.co%2Findex.php%2Fcuadernos-investigacion%2Farticle%2Fdownload%2F1280%2F1159&ei=DmRIVfDCMMigNqvZgeAL&usg=AFQjCNGtSVr54zSt5tAN_Oe34GxNjF5SJg&sig2=p5k4onXUXv9wizDXcLs46w&bvm=bv.92291466,d.eXY

VON SOLMS, Basie. Information Security governance: COBITor ISO 17799 orboth?. Computers& Security, 2005, vol. 24, no 2, p. 99-104.

Guldentops, E. (2002). GoverninginformationtechnologythroughCOBIT. Integrity, Internal Control and Security in InformationSystems (pp. 115-159). SpringerUS.

GUIDE, A. Project Management Body of Knowledge (PMBOK® GUIDE). EnProject Management Institute. 2001.

VERITAS, Grupo Bureau. La organización y cultura de la innovación. Revista Escuela de Administración de Negocios, 2010, no 69, p. 192-201.

ALONSO TORRES, David Hernando, et al. Evaluación de seguridad a sistemas de información en cuanto a ataques maliciosos con base en normatividad, tendencias, impacto y técnicas vigentes para ambientes empresariales a nivel nacional. 2015. Tesis Doctoral.

ICONTEC, Norma Técnica Colombiana. 1486, Presentación de tesis, trabajos de grado y otros trabajos de investigación. Sexta actualización, 2007.
Campo Robledo, J., & Saavedra, J. P. H. (2014). El fraude y la suplantación: Registros mercantiles y sus riesgos. SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO.

16. ANEXOS

16.1 ANEXO A - ACUERDO DE CONFIDENCIALIDAD

Ciudad y Fecha:_____

Yo,

_____

me comprometo a acatar y dar cumplimiento a cada una de las políticas establecidas en el documento POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN y así mismo mantener estricta confidencialidad sobre toda información que por una u otra razón deba conocer como producto del trabajo que actualmente realizo o realizaré.

Firma: _____

Documento de identificación: _____

Empresa: _____

Área de Confecámaras: _____

_____

Vo. Bo. Recursos Humanos

16.2 ANEXO B - AUTODIAGNÓSTICO SEGÚN ANEXO A ISO 27001

AUTODIAGNOSTICO ANEXO A - ISO 27001 - FECHA / PERDIODO: _____ / _____

NUMERAL ISO 27001	CONTROL	¿APLICA?		% CUMPLIMIENTO	SITUACIÓN ACTUAL	OBSERVACIONES
		SI	NO			
1. POLÍTICA DE SEGURIDAD						
1.1. DIRECTRICES DE LA DIRECCIÓN EN SEGURIDAD INFORMÁTICA						
1.1.1	¿Existe un documento formal de políticas aprobado, publicado y comunicado a todos los funcionarios?	SI				
1.12	¿Se revisan periódicamente las políticas y existe un responsable de esta actividad?	SI				
2. ASPECTOS ORGANIZATIVOS SI						
2.1. ORGANIZACIÓN INTERNA						
2.1.1	¿Las responsabilidades de la Seguridad Informática están claramente definidas y asignadas?	SI				
2.1.2	¿Las tareas y las áreas de responsabilidad están debidamente segregadas?	SI				

NUMERAL ISO 27001	CONTROL	¿APLICA?		% CUMPLIMIENTO	SITUACIÓN ACTUAL	OBSERVACIONES
		SI	NO			
2.1.3	¿Los funcionarios encargados de la seguridad mantienen contacto con autoridades?	NO				
2.1.4	¿Los funcionarios encargados de la seguridad mantienen contacto con grupos de interés? (Especialistas, proveedores, colegas y profesionales en seguridad)	SI				
2.1.5	¿La organización aplica los procedimientos de Seguridad Informática previamente establecidos en la gestión de proyectos e independientemente del tipo de proyecto a desarrollar?	SI				
2.2 DISPOSITIVOS PARA MOVILIDAD Y TELETRABAJO						
2.2.1	¿Existe una política para el uso de dispositivos para movilidad?	SI				

NUMERAL ISO 27001	CONTROL	¿APLICA?		% CUMPLIMIENTO	SITUACIÓN ACTUAL	OBSERVACIONES
		SI	NO			
2.2.2	¿Existen políticas y procedimientos implementados para el Teletrabajo?	SI				
3. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS						
3.1 ANTES DE LA CONTRATACIÓN						
3.1.1	¿Se verifican los antecedentes e información presentada por los candidatos a cargos en la organización, contratistas y terceras partes?	SI				
3.1.2	¿Se firman contratos con funcionarios, contratistas y terceras partes, donde se clarifiquen las condiciones del empleo, obligaciones y responsabilidades de seguridad?	SI				
3.2 DURANTE LA CONTRATACIÓN						
3.2.1	¿La alta gerencia exige a los funcionarios, contratistas y terceras partes la aplicación de las políticas y procedimientos de	SI		0%		

NUMERAL ISO 27001	CONTROL	¿APLICA?		% CUMPLIMIENTO	SITUACIÓN ACTUAL	OBSERVACIONES
		SI	NO			
	seguridad?					
7.2.2	¿Los funcionarios, contratistas y terceras partes reciben capacitación, entrenamiento y concientización en seguridad?	SI		0%		
7.2.3	¿Existen procesos disciplinarios para funcionarios por el incumplimiento de las responsabilidades de seguridad?	SI		0%		
3.3 CESE O CAMBIO DE PUESTO DE TRABAJO						
3.3.1	¿Se asignan y definen claramente las responsabilidades por cambio o terminación del contrato?	SI		0%		
4. GESTIÓN ACTIVOS						
4.1 RESPONSABILIDAD SOBRE LOS ACTIVOS						

NUMERAL ISO 27001	CONTROL	¿APLICA?		% CUMPLIMIENTO	SITUACIÓN ACTUAL	OBSERVACIONES
		SI	NO			
4.1.1	¿Existe un Inventario de activos de información críticos para el negocio?	SI				
4.1.2	¿Se han Identificado los propietarios de los activos?	SI				
4.1.3	¿Se han Identificado, documentado e implementado procesos para el uso aceptable de los activos?	SI				
4.1.4	¿Existe un proceso implantado para garantizar el retorno de activos al finalizar contratos y acuerdos? (Funcionarios, contratistas y terceras partes)	SI				
4.2 CLASIFICACIÓN DE LA INFORMACIÓN						
4.2.1	¿Existe una guía para la clasificación de la información en relación a su valor, requisitos legales, sensibilidad y criticidad para la Organización?	SI				

NUMERAL ISO 27001	CONTROL	¿APLICA?		% CUMPLIMIENTO	SITUACIÓN ACTUAL	OBSERVACIONES
		SI	NO			
4.2.2	¿Existe un proceso implementado para el manejo y etiquetado de la información?	SI				
4.2.3	¿Existe un proceso implementado para el manejo, de los activos?	SI				
4.3 MANEJO DE LOS SOPORTES DE ALMACENAMIENTO						
4.3.1	¿Existen procesos implementados para la administración de soportes extraíbles?	SI				
4.3.2	¿Existen procesos implementados destrucción de soportes?	SI				
4.3.3	¿Existen procesos implementados para el transporte seguro de soportes físicos?	SI				
5. CONTROL DE ACCESOS						
5.1 REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESOS						
5.1.1	¿Existe una política de control de acceso?	SI				
5.1.2	¿Existe una política para el uso de la red y de servicios asociados?	SI				
5.2 GESTIÓN DE ACCESO DE USUARIO						

NUMERAL ISO 27001	CONTROL	¿APLICA?		% CUMPLIMIENTO	SITUACIÓN ACTUAL	OBSERVACIONES
		SI	NO			
5.2.1	¿Existe un procedimiento formal de alta y baja de usuarios para habilitar la asignación de derechos de acceso?	SI				
5.2.2	¿Existe un proceso formal implementado para registro de usuarios?	SI				
5.2.3	¿Existe un proceso formal para la administración de privilegios?	SI				
5.2.4	¿Existe un proceso formal para la Gestión de información confidencial de autenticación de usuarios (contraseñas)?	SI				
5.2.5	¿Se revisan periódicamente los privilegios y derechos de acceso de los usuarios?	SI				

NUMERAL ISO 27001	CONTROL	¿APLICA?		% CUMPLIMIENTO	SITUACIÓN ACTUAL	OBSERVACIONES
		SI	NO			
5.2.6	¿Existe un proceso implantado para el retiro de permisos y derechos de acceso al finalizar contratos y acuerdos? (Funcionarios, contratistas y terceras partes)	SI				
5.3 RESPONSABILIDADES DEL USUARIO						
5.3.1	¿Los usuarios siguen buenas prácticas para la selección y el uso de contraseñas?	SI				
5.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES						
5.4.1	¿Se le restringe a los usuarios y personal de mantenimiento el acceso a información y funciones de los sistemas?	SI				
5.4.2	¿Existen implementados procedimientos de inicio seguro de sesión?	SI				
5.4.3	¿Los sistemas de administración de contraseñas permiten implementar contraseñas seguras?	SI				

NUMERAL ISO 27001	CONTROL	¿APLICA?		% CUMPLIMIENTO	SITUACIÓN ACTUAL	OBSERVACIONES
		SI	NO			
5.4.4	¿Se controla el uso de las utilidades de los sistemas críticos?	SI				
5.4.5	¿Se restringe y controla el acceso y uso del código fuente de los sistemas y aplicaciones críticas?	SI				
6. CIFRADO						
6.1 CONTROLES CRIPTOGRÁFICOS						
6.1.1	¿Existen políticas para el uso de controles criptográficos?	SI				
6.1.2	¿Existen procesos formales para administración de llaves criptográficas?	SI				
7. SEGURIDAD FÍSICA Y AMBIENTAL						
7.1 ÁREAS SEGURAS						
7.1.1	¿Se usan esquemas para garantizar un perímetro de seguridad para la plataforma tecnológica y/o sistemas de información críticos?	SI				

NUMERAL ISO 27001	CONTROL	¿APLICA?		% CUMPLIMIENTO	SITUACIÓN ACTUAL	OBSERVACIONES
		SI	NO			
7.1.2	¿Se utilizan controles de entrada para garantizar el acceso de personal autorizado a las áreas seguras?	SI				
7.1.3	¿Se definen e implantan esquemas de seguridad para oficinas, cuartos y edificios?	SI				
7.1.4	¿Se diseñan e implantan esquemas para la protección contra amenazas externas y ambientales?	SI				
7.1.5	¿Se han definido áreas seguras y se han diseñado e implantado controles específicos?	SI				
7.1.6	¿Se controla el acceso a áreas de acceso público, carga y entrega?	SI				
7.2 SEGURIDAD DE LOS EQUIPOS						
7.2.1	¿Los equipos críticos están ubicados y protegidos contra acceso no autorizados?	SI				

NUMERAL ISO 27001	CONTROL	¿APLICA?		% CUMPLIMIENTO	SITUACIÓN ACTUAL	OBSERVACIONES
		SI	NO			
7.2.2	¿Se protegen los equipos contra fallas causadas en los suministros básicos de apoyo?	SI				
7.2.3	¿El cableado y los equipos de comunicaciones están organizados y son protegidos contra interrupción y/o daño?	SI				
7.2.4	¿Se realiza mantenimiento periódico a equipos/dispositivos?	SI				
7.2.5	¿Se controla y autoriza la salida de equipos y/o software de las instalaciones de la organización?	SI				
7.2.6	¿Se protege y controla el acceso a los equipos ubicados fuera de las instalaciones?	SI				
7.2.7	¿Existe un proceso formal implantado para la destrucción y reutilización de equipos o dispositivos?	SI				
7.2.8	¿Se protegen los equipos desatendidos?	SI				

NUMERAL ISO 27001	CONTROL	¿APLICA?		% CUMPLIMIENTO	SITUACIÓN ACTUAL	OBSERVACIONES
		SI	NO			
7.2.9	¿Existe una política de puesto de trabajo despejado y bloqueo de pantalla?	SI				
8. SEGURIDAD DE LAS OPERACIONES						
8.1 RESPONSABILIDADES Y PROCEDIMIENTOS DE OPERACIÓN						
8.1.1	¿Los procedimientos de operación se encuentran documentados?	SI				
8.1.2	¿Existen procesos y/o procedimientos formales para la administración de cambios sobre la plataforma tecnológica y sistemas críticos?	SI				
8.1.3	¿Se monitorea el uso, desempeño y capacidad de los recursos, equipos y sistemas críticos?	SI				
8.1.4	¿Los ambientes de desarrollo, pruebas y producción se encuentran separados?	SI				
8.2 PROTECCIÓN CONTRA CÓDIGO MALICIOSO						

NUMERAL ISO 27001	CONTROL	¿APLICA?		% CUMPLIMIENTO	SITUACIÓN ACTUAL	OBSERVACIONES
		SI	NO			
8.2.1	¿Existen controles implementados en contra de código malicioso?	SI				
8.3 COPIAS DE SEGURIDAD						
8.3.1	¿Se realiza Back-up de información sensible para el negocio?	SI				
8.4 REGISTRO DE ACTIVIDAD Y SUPERVISIÓN						
8.4.1	¿Se generan y almacenan logs de auditoria?	SI				
8.4.2	¿Se protegen los logs de auditoria?	SI				
8.4.3	¿Se monitorean las actividades del administrador y del operador del sistema?	SI				
8.4.4	¿Existe un mecanismo implementado para la sincronización de relojes en los equipos y sistemas críticos?	SI				
8.5 CONTROL DEL SOFTWARE EN EXPLOTACIÓN						
8.5.1	¿Existen controles para la instalación de software y sistemas operativos?	SI				
8.6 GESTIÓN DE LA VULNERABILIDAD TÉCNICA						

NUMERAL ISO 27001	CONTROL	¿APLICA?		% CUMPLIMIENTO	SITUACIÓN ACTUAL	OBSERVACIONES
		SI	NO			
8.6.1	¿Existe un proceso/procedimiento para identificar, evaluar y controlar vulnerabilidades técnicas sobre los sistemas de información críticos para el negocio?	SI				
8.6.2	¿Existen controles y políticas para la instalación de software por parte de los usuarios?	SI				
8.7 CONSIDERACIONES DE LAS AUDITORÍAS DE LOS SISTEMAS DE INFORMACIÓN						
8.7.1	¿Se planean y controlan las actividades de revisión realizadas por auditorías a sistemas de procesamiento para minimizar riesgos y evitar fallas en sistemas críticos?	SI				
9. SEGURIDAD EN LAS TELECOMUNICACIONES						
9.1 GESTIÓN DE LA SEGURIDAD EN LAS REDES						
9.1.1	¿Se tienen implementados controles en las redes de datos?	SI				

NUMERAL ISO 27001	CONTROL	¿APLICA?		% CUMPLIMIENTO	SITUACIÓN ACTUAL	OBSERVACIONES
		SI	NO			
9.1.2	¿Se identifican e incluyen requerimientos y niveles de servicio sobre las redes internas y/o externas?	SI				
9.1.3	¿Existe una adecuada Segmentación de redes, de acuerdo al tipo de usuarios, servicios y sensibilidad de los sistemas de información?	SI				
9.2 INTERCAMBIO DE INFORMACIÓN CON PARTES EXTERNAS						
9.2.1	¿Existen políticas y procedimientos para el intercambio de información?	SI				
9.2.2	¿Existen acuerdos para el intercambio de información con terceras partes?	SI				
9.2.3	¿Existen controles de seguridad para la protección de la mensajería electrónica?	SI				

NUMERAL ISO 27001	CONTROL	¿APLICA?		% CUMPLIMIENTO	SITUACIÓN ACTUAL	OBSERVACIONES
		SI	NO			
9.2.4	¿Existen acuerdos de confidencialidad firmados con funcionarios y terceros con acceso a información sensible para el negocio?	SI				
10. AQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN						
10.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN						
10.1.1	¿Se identifican y analizan los requerimientos de seguridad no solo para nuevos sistemas de información sino también para mejoras a los ya existentes?	SI				
10.1.2	¿Se han implementado controles para los servicios de aplicación que pasan a través de redes públicas?	SI				
10.1.3	¿Se protegen las transacciones por redes telemáticas?	SI				
10.2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE						

NUMERAL ISO 27001	CONTROL	¿APLICA?		% CUMPLIMIENTO	SITUACIÓN ACTUAL	OBSERVACIONES
		SI	NO			
10.2.1	¿Existen políticas para el desarrollo seguro de software y sistemas dentro de la organización?	SI				
10.2.2	¿Existen procesos y/o procedimientos formales para el control de cambios sobre la plataforma tecnológica y sistemas críticos?	SI				
10.2.3	¿Se realizan revisiones y pruebas a las aplicaciones y sistemas de información críticos para el negocio, luego de hacer cambios sobre los sistemas operativos?	SI				
10.2.4	¿Se identifican, restringen y controlan los cambios a paquetes de software comerciales instalados en ambientes críticos?	SI				

NUMERAL ISO 27001	CONTROL	¿APLICA?		% CUMPLIMIENTO	SITUACIÓN ACTUAL	OBSERVACIONES
		SI	NO			
10.2.5	¿El área de Sistemas de la Organización aplica los principios de ingeniería de sistemas en la implementación de cualquier sistema de información?	SI				
10.2.6	¿Existen políticas para establecer y proteger adecuadamente los entornos para las labores de desarrollo e integración de sistemas que abarcan todo el ciclo de vida de desarrollo del sistema?	SI				
10.2.7	¿Se revisa, monitorea y controla el software desarrollado por terceros?	SI				
10.2.8	¿Existen procedimientos definidos para la realización de pruebas de funcionalidad durante el desarrollo de un	SI				

NUMERAL ISO 27001	CONTROL	¿APLICA?		% CUMPLIMIENTO	SITUACIÓN ACTUAL	OBSERVACIONES
		SI	NO			
	sistema?					
10.2.9	¿Existen criterios claros y procedimientos para la aceptación y prueba de nuevos sistemas de información?	SI				
10.3 DATOS DE PRUEBA						
10.3.1	¿Existen controles para la selección y protección de los datos usados en ambientes de pruebas?	SI				
11. RELACIONES CON LOS PROVEEDORES						
11.1 SEGURIDAD INFORMÁTICA EN LAS RELACIONES CON SUMINISTRADORES						
11.1.1	¿Se han implementado controles en la entrega de servicios de terceras partes?	SI				
11.1.2	¿Los requisitos de seguridad informática con proveedores que deban acceder a los servicios y/o a la información de la organización, están debidamente	SI				

NUMERAL ISO 27001	CONTROL	¿APLICA?		% CUMPLIMIENTO	SITUACIÓN ACTUAL	OBSERVACIONES
		SI	NO			
	establecidos y acordados?					
11.1.3	¿Están incluidos en los acuerdos con proveedores los respectivos requisitos para abordar los riesgos de la seguridad de la información asociada con los servicios de las tecnologías de información y comunicación y de la cadena de suministro de productos?	SI				
11.2 GESTIÓN DE LA PRESTACIÓN DEL SERVICIO POR SUMINISTRADORES						
11.2.1	¿Se monitorean y revisan los servicios prestados por terceras partes?	SI				
11.2.2	¿Se administran los cambios en los servicios prestados por terceras partes?	SI				
12. GESTIÓN DE INCIDENTES						
12.1 GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA Y MEJORAS						

NUMERAL ISO 27001	CONTROL	¿APLICA?		% CUMPLIMIENTO	SITUACIÓN ACTUAL	OBSERVACIONES
		SI	NO			
12.1.1	¿Se han establecido responsabilidades y procedimientos para asegurar una rápida y efectiva respuesta ante incidentes de seguridad?	SI				
12.1.2	¿Existen canales y/o procedimientos para reportar eventos de seguridad?	SI				
12.1.3	¿Se le solicita a funcionarios y terceros observar y reportar debilidades de seguridad en servicios y sistemas?	SI				
12.1.4	¿Existe un procedimiento para evaluar los eventos de Seguridad Informática ocurridos al interior de la Organización?	SI				

NUMERAL ISO 27001	CONTROL	¿APLICA?		% CUMPLIMIENTO	SITUACIÓN ACTUAL	OBSERVACIONES
		SI	NO			
12.1.5	¿Existe un Plan de Continuidad del Negocio para dar una respuesta efectiva de funcionarios y procesos en caso de contingencia o eventos catastróficos que se presenten en la misma y que afecten la continuidad de su operación?	SI				
12.1.6	¿Existen mecanismos para calificar, monitorear y aprender de los incidentes de seguridad registrados?	SI				
12.1.7	¿Existen procesos formales para la recolección, retención y entrega de evidencia ante entes legales?	SI				
13. ASPECTOS DE LA SI EN LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO						
13.1 CONTINUIDAD DE LA SEGURIDAD INFORMÁTICA						
13.1.1	¿Se han determinado los requisitos de Seguridad Informática ante una situación de	SI				

NUMERAL ISO 27001	CONTROL	¿APLICA?		% CUMPLIMIENTO	SITUACIÓN ACTUAL	OBSERVACIONES
		SI	NO			
	crisis o desastre?					
13.1.2	¿Se han establecido los procesos, procedimientos y controles para garantizar el nivel necesario de Seguridad Informática durante situaciones adversas?	SI				
13.1.3	¿El plan de continuidad es probado y actualizado regularmente?	SI				
13.2 REDUNDANCIAS						
13.2.1	¿Existe una plataforma tecnológica redundante que satisfaga los requerimientos de disponibilidad aceptables para la misma?					
14. CUMPLIMIENTO						
14.1 CUMPLIMIENTO DE LOS REQUISITOS LEGALES Y CONTRACTUALES						

NUMERAL ISO 27001	CONTROL	¿APLICA?		% CUMPLIMIENTO	SITUACIÓN ACTUAL	OBSERVACIONES
		SI	NO			
14.1.1	¿Se han identificado y documentado los requerimientos de seguridad exigidos por las leyes, regulaciones y obligaciones contractuales aplicables a los sistemas y a la organización?	SI				
14.1.2	¿Existen procedimientos implementados para garantizar los derechos de propiedad intelectual y el uso de productos de software?	SI				
14.1.3	¿Se protegen los registros físicos y lógicos importantes para el negocio, evitando su perdida, destrucción, modificación o falsificación?	SI				
14.1.4	¿Se protege la privacidad de la información personal de los funcionarios y de los afiliados?	SI				

NUMERAL ISO 27001	CONTROL	¿APLICA?		% CUMPLIMIENTO	SITUACIÓN ACTUAL	OBSERVACIONES
		SI	NO			
14.1.5	¿Se utilizan controles criptográficos para cumplir con acuerdos, leyes o regulaciones?	SI				
14.2 REVISIONES DE LA SEGURIDAD INFORMÁTICA						
14.2.1	¿Los objetivos de control, controles, políticas, procesos y procedimientos de Seguridad Informática implementados son afines al enfoque de la organización?	SI				
14.2.2	¿Los gerentes de área fomentan e implantan esquemas para asegurar el cumplimiento de las políticas y procedimientos de seguridad corporativos?	SI				
14.2.3	¿Los sistemas de información críticos son probados técnicamente para verificar el cumplimiento de los requerimientos de seguridad?	SI				