DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BAJO LA NORMA ISO 27001:2013 PARA LA EMPRESA UNISANAR IPS DE QUIBDÓ

LETTY YANETH MORENO PALOMEQUE
YACIRY ENITH PALACIOS PALACIOS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
QUIBDÓ, CHOCÓ
2018

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BAJO LA NORMA ISO 27001:2013 PARA LA EMPRESA UNISANAR IPS DE QUIBDÓ

LETTY YANETH MORENO PALOMEQUE
YACIRY ENITH PALACIOS PALACIOS

Trabajo de grado para optar por el título:
Especialista en Seguridad Informática

Director de Proyecto:
Ing. Daniel Felipe Palomo Luna

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
QUIBDÓ, CHOCÓ
2018

Nota de Aceptación:

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Quibdó, 13 de Febrero 2018

DEDICATORIA

Esta monografía se la dedicamos a nuestra familia, quienes con su apoyo y voz de aliento supieron acompañarnos en este proceso, de igual forma a todas las personas que nos brindaron su confianza y exaltan día a día nuestra labor.

AGRADECIMIENTOS

Esta meta no podría ser realidad sin Dios todopoderoso, quien ha permitido nuestra llegada hasta este punto, a nuestras familias, a nuestros padres por su voz de aliento, amigos y allegados por su apoyo constante y motivación, sin dejar de lado a los funcionarios de la empresa UNISANAR IPS, por su disposición y acompañamiento; por ultimo pero sin ser menos importante a los ingenieros directores por su guía, seguimiento y constante retroalimentación durante todo este proceso, mil y mil gracias a todos.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE ILUSTRACIONES

pág.

LISTA DE ANEXOS

pág.

GLOSARIO

ACTIVOS: Es un recurso, proceso, producto o sistema que tiene algún valor para la organización y por lo tanto debe ser protegido.

ADMINISTRACIÓN DE RIESGOS: Se llama así al proceso de identificación, análisis y evaluación de riesgos.

AMENAZA: Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización.

ANÁLISIS DE REQUISITOS: consiste en estudiar los requerimientos de seguridad de la información para el proceso SGSI bajo la normativa ISO/IEC 27001 definidos.

ANÁLISIS: Investigación objetiva y cuidadosa de dato, transformado para su estudio.

CICLO PDCA: Viene de las siglas Planificar, Hacer, Verificar y Actuar, en inglés "Plan, Do, Check, Act". Describe los cuatro pasos esenciales que se deben llevar a cabo de forma sistemática para lograr la mejora continua, entendiendo como tal al mejoramiento continuado de la calidad (disminución de fallos, aumento de la eficacia y eficiencia, solución de problemas, previsión y eliminación de riesgos potenciales…).

CICLO PHVA: Es una herramienta de la mejora continua, presentada por Deming a partir del año 1950, la cual se basa en un ciclo de 4 pasos: Planificar (Plan), Hacer (Do), Verificar (Check) y Actuar (Do).

CMMI (EN INGLÉS CAPABILITY MATURITY MODEL INTEGRATION, INTEGRACIÓN DE MODELOS DE MADUREZ DE LAS CAPACIDADES): Es un

proceso enfoque de mejoramiento que proporciona a las organizaciones los elementos esenciales de los procesos.

CONFIDENCIALIDAD: Garantizar que la información es accesible sólo para aquellos usuarios autorizados a tener acceso.

CPD: Se denomina centro de procesamiento de datos, aquel espacio donde se concentran los recursos necesarios para el procesamiento de la información de una organización.

DATOS: Es una representación simbólica (numérica, alfabética, algorítmica, etc.) de un atributo o variable cuantitativa. Es un valor o referente que recibe el computador por diferentes medios, los datos representan la información que el programador manipula en la construcción de una solución o en el desarrollo de un algoritmo.

DEBILIDAD: Se refieren a todos aquellos elementos, recursos, habilidades y actitudes que la empresa ya tiene y que constituyen obstáculos para lograr la buena marcha de la organización.

DECLARACIÓN DE APLICABILIDAD (INGLES: STATEMENT OF APPLICABILITY; SOA): Documento donde se encuentran enumerados los controles que se aplican el Sistema de Gestión de Seguridad de la Información de una empresa, luego de haber realizado la evaluación y tratamiento de riesgo al igual de las exclusiones de controles del Anexo A de ISO 27001:2013.

DISPONIBILIDAD: Garantiza contar con la información en el momento y tiempo requerido.

DROPBOX: Es un servicio online que permite almacenar archivos en la nube, permitiendo también compartir archivos y carpetas con otros usuarios. Sus servicios son: almacenamiento en la nube, sincronización de archivos, nube personal y software cliente.

INFORMACIÓN: Son todos aquellos datos organizados y convenientemente procesados que nos permiten extraer el conocimiento que facilita la toma de decisiones, permitiendo el seguimiento de los objetivos propuestos mediante una actuación apropiada.

INTEGRIDAD: Garantiza que la información permanezca completa y no sea alterada de manera NO autorizada.

NIVELES DE MADUREZ: Conjunto predefinido de áreas de proceso. Los niveles de madurez se miden por el logro de los objetivos genéricos y específicos que se aplican a cada conjunto predefinido de áreas de proceso.

NO REPUDIO: Es la prevención de la negación de un servicio que es enviado o recibido y asegura que las partes involucradas no pueda negar que lo envió o que el receptor se rehúse haberlo recibido.

NORMA ISO: Sigla de la expresión inglesa International Organization for Standardization, 'Organización Internacional de Estandarización', sistema de normalización internacional para productos de áreas diversas. Pauta definida por la Organización Internacional de Normalización que se aplica a los productos y servicios.

POLÍTICAS: Estándares de Seguridad Informática.

RIESGOS: Combinación de la probabilidad de un evento y su consecuencia.

SISTEMA: Conjunto de reglas, principios o medidas que tienen relación entre sí.

SLA (SERVICE LEVEL AGREEMENT): Es un contrato que describe el nivel de servicio que un cliente espera de su proveedor. En español, también se llama Acuerdo de Nivel de Servicio (ANS).

VULNERABILIDAD: Es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las inseguridades pueden aparecer en cualquiera de los partes de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.

INTRODUCCIÓN

La seguridad es un proceso de mejora continua por lo que las políticas y procedimientos establecidos para la protección de la información deberán revisarse y adecuarse, de ser necesario, ante los nuevos riesgos que puedan surgir eventualmente, a fin de tomar las acciones que permitan reducirlos y en el mejor de los casos eliminarlos.

En el presente documento se desarrollará el diseño del Sistema de Gestión de Seguridad de la Información – SGSI, se propone establecer los procedimientos y políticas de seguridad de la información dentro de la organización, las cuales deben ser sustentadas por organismos que avalen la correcta implementación de dichos procedimientos.

Con el fin de garantizar la seguridad de los activos que se encuentran en UNISANAR IPS, se hace necesario el diseño de un Sistema De Gestión De Seguridad De La Información (SGSI), así se podrá comenzar a evaluar la importancia de proteger la información por medio de la implementación y sea de acceso único de las personas responsables o autorizadas. Buscando que se proteja la información y que el acceso sea únicamente para las personas autorizadas.

Para lograr un buen éxito en el proceso de seguridad de la información, se requiere tener un diseño del Sistema de Información haciendo uso del ciclo PHVA (Planear, Hacer, Verificar y Actuar).[1]

Los sistemas de Gestión se basan en normas enfocadas a mejorar los procesos dentro de las organizaciones. Se destacan las normas emitidas por la Organización Internacional de Estandarización (ISO) en relación con la implantación de sistemas

[1] Norma Técnica Colombiana NTC-ISO/IEC 27001:2013

de gestión a través de la familia de Normas ISO/IEC 27001. Las investigaciones internacionales y nacionales han tenido por objetivo principal, estudiar cuál ha sido la motivación que ha llevado a las empresas a implantar el modelo ISO/IEC 27001 y cuáles han sido las dificultades detectadas. Se ha tratado de establecer los beneficios que la implantación de esta normativa ha producido en las empresas.

En consecuencia, la seguridad consta de tres elementos fundamentales que forman parte de los objetivos que intentan comprometer los atacantes: La confidencialidad, la integridad y la disponibilidad de los recursos. Por lo que deben existir procedimientos y mejores prácticas que faciliten la lucha contra las actividades delictivas y reducen notablemente el campo de acción de los ataques, motivos por los que se hace necesario diseñar un sistema de gestión de seguridad de la información (SGSI) bajo la norma ISO 27001:2013.

1 PLANTEAMIENTO DEL PROBLEMA

UNISANAR I.P.S., es una mediana empresa del área de la salud, que presta servicios médicos de baja complejidad en el departamento del Chocó; con más de 10 años de existencia, viene presentando un proceso de crecimiento continuo en su participación como IPS privada, que presta servicios a usuarios del régimen subsidiado, contributivo y particulares que requieran de atención medica general, servicios de hospitalización, odontológicos, curaciones, imágenes diagnósticas, farmacia, atención medica domiciliaria.

Esto ha permitido que, entre sus más de 20.000 pacientes, y alrededor de 72.000 consultas, se cuente con unos pacientes de condiciones clínicas especiales, que presentan enfermedades virales muy contagiosas y de manejo reservado.

Debido a la gran cantidad de pacientes/usuarios, posee un flujo de información creciente, que demanda año a año, mayor espacio para el almacenamiento y conservación en el archivo físico de historias clínicas, generando el uso ineficiente de algunos espacios físicos, del área administrativa de la empresa.

Por este motivo, la gerencia de UNISANAR IPS, decidió almacenar la información de las historias clínicas de todos los usuarios de manera ordenada, procediendo con el almacenamiento sistematizado de las historias clínicas de los pacientes con diagnóstico de enfermedades contagiosas como, VIH, TUBERCULOSIS, VENEREAS, LEPRA, y otras, cuyo manejo exige la mayor discreción por parte del personal asistencial y administrativo que conozca de su diagnóstico, así como disponibilidad de la información para la toma de decisiones y rendición de informes a las autoridades sanitarias.

Si bien la sistematización de la información, permite un manejo ágil, accesible, organizado, controlado y duradero de la misma, disminuyendo los costos administrativos del personal de archivo, y haciendo más eficiente la gestión documental de UNISANAR IPS, esto trajo consigo también que cualquier usuario de los equipos de cómputo pueda acceder fácilmente a la información, manipularla, publicarla o usarla en fines diferentes a los permitidos por la normatividad vigente actualmente en salud, y colocando en riesgo la estabilidad administrativa, financiera y legal de UNISANAR IPS.

Conociendo que UNISANAR IPS, basa todo su accionar administrativo y asistencial en el manejo sistematizado de la información, y con la utilización de la red LAN (Local Área Network) como vía para compartir Software, Hardware y todo tipo de información de manera interna y externa, es importante que se implementen estrategias de controles y medidas, que permitan o ayuden a minimizar, la vulnerabilidad y riesgos a los que se exponen ante intrusos que deseen acceder a la información privilegiada, con el ánimo de alterarla, hurtarla o usarla con finalidades distintas a la destinación dada por la empresa, preservando así, la seguridad de la red, fallas en los sistemas de información, caída de red, y prevenir mal funcionamiento de Hardware y/o Software.

Si UNISANAR IPS, no implementa la ISO/IEC 27001, se hará más complejo la identificación de la amenazas a las que se ve expuesta, así como no se lograra efectuar los posibles controles ante los niveles de riesgos que se detecten, como son: hurto de la información, fallos en los sistemas, e instalación de procesos y procedimientos que reglamenten el uso de su red LAN de manera segura, produciendo una filtración de la información confidencial de la IPS, afectando a los usuarios y clientes, y colocando en riesgo la confidencialidad de la información privilegiada que administra, generando desconfianza y poca credibilidad en sus servicios.

Durante dos (2) meses se analizará en las instalaciones centrales de UNISANAR IPS, el flujo de información, la forma en que es almacenada, los usuarios autorizados para almacenarla, las fuentes que proveen la información, y el uso final que se da a la misma, determinando el nivel del riesgo a que está sometida.

2 FORMULACIÓN DEL PROBLEMA

¿El diseño de un sistema de gestión de seguridad de la información, podría apoyar a UNISANAR IPS, para la implementación de controles de seguridad que mitiguen los riesgos de perdida de información, entre otros, que puedan afectar la integridad, confiabilidad y disponibilidad de la información de la entidad?

3 JUSTIFICACIÓN

Mediante este proyecto, se podrá determinar el estado actual de la seguridad de la información, un análisis de riesgos y una recomendación de implementación de controles que se ciñan a las normas ISO 27001:2013.

Con lo anterior se pretende mejorar la calidad del servicio que brinda la empresa, así se mantendrá el control adecuado a cada uno de los procesos que se realizan en UNISANAR IPS, evitando vulnerabilidades, manipulación y modificación de la información, por usuarios, empleados, o ante ataques de hackers, crackers o cualquier tipo de amenazas informáticas y así garantizar la confidencialidad, disponibilidad e integridad de la información, manteniéndola fuera del alcance de cualquier tipo de intruso, sea interno o externo.

Cuando UNISANAR IPS, decida implementar el Sistema de Gestión de Seguridad de la Información, bajo el conjunto de los estándares de la ISO 27001:2013, le permitirá garantizar que los usuarios, clientes, proveedores y la sociedad Quibdoseña en general, tengan la certeza que la información privilegiada que ha sido entregada a UNISANAR IPS, sea usada de acuerdo a la normatividad vigente, garantizando su confidencialidad, integridad y disponibilidad, generando cohesión social, y aumentando el nivel de satisfacción y confianza de cada uno de los beneficiarios de los servicios prestados por la IPS.

4 OBJETIVOS

4.1 GENERAL

Diseñar un Sistema de Gestión de Seguridad de la Información para UNISANAR IPS, bajo la norma ISO 27001:2013, que le permita implementar la seguridad de la información y establecer las medidas preventivas y correctivas necesarias; para garantizar la confidencialidad, integridad y disponibilidad de la información administrada por la IPS.

4.2 ESPECÍFICOS

- Diagnosticar la situación actual de la seguridad de la información de acuerdo con el anexo A de la norma ISO 27001:2013 en UNISANAR IPS.

- Realizar un levantamiento de activos de información en UNISANAR IPS.

- Realizar un análisis de riesgos de acuerdo con los activos encontrados en UNISANAR IPS

- Proponer los controles de seguridad aplicables de la norma ISO 27001:2013

- Plantear políticas de seguridad de la información aplicables para UNISANAR IPS.

5 MARCO REFERENCIAL

5.1 MARCO TEÓRICO

Actualmente nos encontramos en la era de la información y el conocimiento, las organizaciones deben tener como uno de sus principales objetivos el cuidado, seguridad y disponibilidad de sus activos de información; sin la adecuada preservación de la información de una empresa, esta perderá aquellas ventajas que la hacen ser competitiva y terminara por desaparecer del mercado; porque entre más tecnología y reconocimiento en las organizaciones mayor es el riesgo de la información si no existe protección contra amenazas y vulnerabilidades.

Para una adecuada gestión de la información es necesario implantar una metodología rigurosa y clara, que con base en normas preestablecidas le permitan a cualquier individuo de la organización asegurar la disponibilidad y seguridad de la información que maneja.

5.2 SISTEMA DE GESTIÓN

Es el encargado de la implementación de los procesos que ayudan a que una organización ejecute servicios o productos de forma confiable y acorde a las especificaciones internacionales.[2]

[2] Sistema de gestión de seguridad de la información, ISO 27001 Elaborado: Centro Europeo de empresas de innovación Albacete (2010)

5.3 NORMATIVAS DE GESTIÓN DE LA SEGURIDAD

Son los lineamientos precisos para que una organización pueda orientar, planear, diseñar e implantar un SGSI (Sistema de Gestión de la Seguridad de la Información); el cual se realiza mediante un proceso y una serie de fases donde se puede definir los mecanismos principales de seguridad documentada y conocida por los integrantes de la organización.

Es importante que se sepa que la implementación de SGSI (Sistema de Gestión de la Seguridad de la Información) no es garante de la protección máxima ya que su intención es que los riesgos de la seguridad de la información sean detectados, obtenidos, tratados y contrarrestados en la organización, dejando todo documentado, sistematizado, ordenado, eficiente y adaptable a los cambios que se vayan generando en la detección de riesgos, en el ambiente y las tecnologías.

El SGSI (Sistema de Gestión de la Seguridad de la Información), está constituido por unas normas tales como:

Normativas que abarcan las buenas prácticas para la seguridad de la información, en las cuales se encuentran los códigos de buenas prácticas que sirven para que las empresas la utilicen para mejorar la seguridad de su información.

Normativas que involucran las especificaciones de los SGSI, que sería la documentación que deben tener las empresas que deseen certificarse su SGSI (Sistema de Gestión de la Seguridad de la Información).[3]

[3] Tomado del módulo curso 233003 de sistema de gestión de seguridad de la información SGSI UNAD 2013

5.4 NORMA ISO

La *International Organization for Standardization* - ISO e International Electrotechnical Commission – IEC, desarrollaron la familia de Normas ISO/IEC 27000, donde se proporcionan los lineamientos para la gestión de la seguridad en la información en cualquier empresa.

5.5 NORMA ISO 27000

Gestión de la seguridad de la información (Fundamentos y vocabulario). Esta norma fue publicada el 1 de mayo de 2009 y contemplan en forma introductoria todos los aspectos fundamentales que enfoca un sistema de gestión de seguridad de la información (SGSI), una descripción del ciclo PDCA (del inglés ***plan-do-check-act***, esto es, planificar-hacer-verificar-actuar), al igual que las definiciones de los términos que se emplean en toda la serie 27000, esta norma tiene una similitud con las normas de Gestión de Calidad ISO 9000, son una serie de estándares con un rango que va de la 27000 a 27019 y de 27030 a 27044, pero en este documento se describen hasta 27007. Cada una de las normas de la familia 27000, precisa y concentra todos los aspectos trascendentales de la gestión de la seguridad de la información en cualquier empresa pequeña, mediana o grande, así como públicas y privadas.

5.5.1 Objetivos. Esta familia de normas que tiene como objetivo definir requisitos para un sistema de gestión de la seguridad de la información (SGSI), con el fin de garantizar la selección de controles de seguridad adecuados y proporcionales, protegiendo así la información, es recomendable para cualquier empresa grande o pequeña de cualquier parte del mundo y más especialmente para aquellos sectores que tengan información crítica o gestionen la información de otras empresas.

5.5.2 Familia 27000.

5.5.2.1 *ISO/IEC 27001:* Es la norma más importante de la familia 27001 porque abarca todos los requisitos pertinentes que se deben tener en cuenta en el sistema de gestión de seguridad de la información. Cuenta con un Anexo A, que detalla de manera resumida los objetivos de los dominios con sus respectivos controles que explica la ISO 27001:2005, con la finalidad de que en las organizaciones se implemente en el desarrollo de los SGSI.

Fue Publicada el 15 de Octubre de 2005, revisada el 25 de Septiembre de 2013, y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está escrita por especialistas en el tema y suministra una técnica para implementar el Sistema de Gestión de la Seguridad de la Información en una organización. Así mismo permite que una empresa sea certificada; o sea que una entidad certificada fue implementada en cumplimiento bajo la norma ISO 27001.

5.5.3 Los beneficios que se obtiene en la utilización de la norma ISO 27001: Para el cumplimiento de los requisitos legales, la mejor opción es la norma ISO 27001, ya que esta se encuentra en la actualidad con la mejor metodología, garantizando mayor cumplimiento y mejores respuestas.

Al conseguir una certificación comercial, se convierte de gran utilidad ante los ojos de los clientes, toda vez que una empresa certificada genera mayor confiabilidad a la hora de preservar la información, dando mejores ventajas ante las otras organizaciones.

Menos costos; contrarresta incidentes de seguridad, lo que evita costos y ahorra gastos.

Organización y claridad en los procesos y procedimientos de la empresa, dejando claro las funciones, responsables y acciones a tomar, con miras a aumentar la motivación de sus empleados por tener directrices claras y coherentes. [4]

5.5.4 ¿Cómo funciona la ISO 27001? Esto se hace mediante la evaluación de riesgos, analizando los potenciales problemas que pueden llegar a afectar la información, posteriormente se definen las acciones a tomar para minimizar los riesgos de manera sistemática.

Los controles que se deben implementar se presentan, por lo general, bajo la forma de políticas, procedimientos e implementación técnica (por ejemplo, software y equipos). Sin embargo, en la mayoría de los casos, las empresas ya tienen todo el hardware y software, pero lo utilizan de una forma no segura; por lo tanto, la mayor parte de la implementación de ISO 27001 estará relacionada con determinar las reglas organizacionales (por ejemplo, redacción de documentos) necesarias para prevenir violaciones de la seguridad, es por ello que la seguridad de la información no se limita a lo relacionado con las TI (Tecnologías de la Información) solamente, sino que además va de la mano con la gestión de procesos, de los recursos humanos, con la protección jurídica, la protección física, etc.[5]

[4] http://www.eoi.es/blogs/ciberseguridad/2016/06/10/la-normativa-iso-27001-analisis-de-situacion-en-las-organizaciones/

[5] http://www.eoi.es/blogs/ciberseguridad/2016/06/10/la-normativa-iso-27001-analisis-de-situacion-en-las-organizaciones/

5.5.4.1 ISO/IEC 27002: En esta norma es una enseñanza de los pasos a seguir, explica los objetivos de los dominios y controles que son convenientes cuando se habla de seguridad de la información. Cuenta con 39 Objetivos y 133 controles, asociados en 11 dominios.

Publicada desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición.

Esta norma no certificable, es una guía de buenas prácticas que detalla los objetivos de control y controles recomendables en los aspectos de seguridad de la información. En cuanto a seguridad de la información. Esta norma se encuentra publicada en español a través de la empresa AENOR y en Colombia NTC -ISO IEC 27002), así mismo se pueden encontrar en Perú, chile, entre otros países latinoamericanos.[6]

5.6 SEGURIDAD DE LA INFORMACIÓN

La información representa valor para las organizaciones; por lo tanto, es un activo ya que es un conjunto de datos, es esencial para el negocio de una organización, y en consecuencia es necesario asegurar su protección.

Como resultado del crecimiento tecnológico y la globalización, la información ahora está expuesta a un número cada vez mayor y una variedad más amplia de amenazas y vulnerabilidades. La información puede existir en muchas formas: puede estar impresa o escrita en un papel, almacenada en magnético, enviada por correo o utilizando medios electrónicos, videos o grabaciones de voz. Sin importar la forma que tome la información, o medio por el cual sea almacenada o compartida, siempre debe estar protegida.

[6] Tomado del módulo curso 233003 de sistema de gestión de seguridad de la información SGSI UNAD 2013

La seguridad de la información es la protección de los datos, de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales. Existen tres clases de grupo de amenazas a la que se encuentra expuesta el recurso más importante de la organización (los datos):

Externas: Intrusión a las redes de la organización o instalaciones físicas, por ejemplo: spam, hackers, suplantación de identidad, fraude, espionaje, sabotaje, robo de información, entre otras.

Internas: Generadas al interior de la organización, principalmente por el conocimiento de los colaboradores. Ejemplo: Alteración de la información, divulgación de la información, fraudes, robo, sabotaje, uso no autorizados de sistemas informáticos, uso de imagen corporativa sin autorización, etc.

Naturales: Generadas por desastres naturales, como inundaciones, huracanes, terremotos, incendios, etc.

Como lo resalta la ISO 27002:2005: La seguridad de la información se logra implementando un adecuado conjunto de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Se necesitan establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de seguridad y comerciales específicos. Esto se debiera realizar en conjunción con otros procesos de gestión del negocio.

5.7 NECESIDAD DE LA SEGURIDAD DE LA INFORMACIÓN

(BUITRAGO ESTRADA, y otros, 2015) Establecer, documentar, implementar y mantener el Sistema de Gestión de Seguridad de la Información es importante para las organizaciones al representar una ventaja competitiva, flujo de caja, productividad, rentabilidad, estatus en el mercado y cumplimiento legal; al asegurar que la información, los procesos, la imagen corporativa y sistemas de apoyo son activos comerciales importantes.

Los activos de información de las organizaciones enfrentan amenazas de seguridad entre ellas: fraude por internet, espionaje, sabotaje, hurto, fenómenos naturales, fuego o inundación. Las causas de daño como código malicioso, spam o hackers se hacen cada vez más comunes, más efectivas, más ambiciosas y cada vez más sofisticadas. De acuerdo con esto, la seguridad de la información es importante para todas las unidades de negocio sin importar que pertenezcan al sector público o privado.

En el mercado existe una variedad de software diseñados para ser seguros, aunque continúan presentándose amenazas y vulnerabilidades en la información, por esto es importante un trabajo integrado con la gestión y procedimientos adecuados, que permitan identificar qué controles son necesarios, lo cual se alcanza con la planeación, hacer, verificar y actuar del SGSI. La gestión de la seguridad de la información requiere, como mínimo, la participación de todos los grupos de interés de la organización. Además, es conveniente requerir asesoría especializada de organizaciones externas.

Según la norma ISO 27002 de 2005 es esencial que una organización identifique sus requerimientos de seguridad. Existen tres fuentes principales de requerimientos de seguridad:

Una fuente se deriva de evaluar los riesgos para la organización, tomando en cuenta la estrategia general y los objetivos de la organización. A través de la evaluación del riesgo, se identifican las amenazas para los activos, se evalúa la vulnerabilidad y la probabilidad de ocurrencia y se calcula el impacto potencial.

Otra fuente son los requerimientos legales, reguladores, estatutarios y contractuales que tienen que satisfacer una organización, sus socios comerciales, contratistas y proveedores de servicio; y su ambiente sociocultural.

Otra fuente es el conjunto particular de principios, objetivos y requerimientos comerciales para el procesamiento de la información que una organización ha desarrollado para sostener sus operaciones.[7]

5.8 PLAN DE GESTIÓN DE UN SGSI

La ISO 27001, expresa que un Sistema de Gestión de la Seguridad de la información, es un sistema de gestión que comprende la política, estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información. Este sistema es la herramienta de que dispone la Dirección de las organizaciones para llevar a cabo las políticas y los objetivos de seguridad (integridad, confidencialidad y disponibilidad, asignación de responsabilidad, autenticación, etc.). Este sistema proporciona mecanismos para la salvaguarda de los activos de información y de los

[7] BUITRAGO ESTRADA, Johanna Carolina, BONILLA PINEDA, Diego Hernando y MURILLO VARON, Carol Estefanie. 2015. Diseño de una metodología para la implementación del sistema de gestión de seguridad de la información - SGSI, en el sector de laboratorios de análisis microbiológicos, basado en ISO 27001. [En línea] 2015. http://repository.ean.edu.co/bitstream/handle/10882/2692/MurilloCarol2012.pdf?sequence=1.

sistemas que los procesan, en concordancia con las políticas de seguridad y planes estratégicos de la organización[8]

5.8.1 ¿Cómo definir el alcance del SGSI? La planeación para la implementación de un SGSI es una etapa ineludible, por tanto, definir el alcance para la implementación del sistema en una organización es uno de los primeros aspectos que se debe considerar. Teniendo en cuenta que existen organizaciones que difieren en tamaño por el número de empleados, volumen de información manejada, número de clientes, volúmenes de activos físicos y lógicos, número de sedes u oficinas, entre otros elementos, se hace necesario determinar qué áreas o dependencias de la organización se desea implantar el SGSI como primera medida y cuales posteriormente. Las primeras áreas que se deben considerar son aquellas que por sus funciones y responsabilidades ayudan en primera instancia a dar cumplimiento a la misión institucional.

Se puede considerar, por ejemplo, una empresa comercial de compra y venta de productos para la construcción, los cuales comercializan por internet, y de manera presencial en sus diferentes sedes locales y nacionales. En tal sentido, se puede apreciar, que una empresa de este estilo o tipo puede ser de tamaño mediano o alto, por tanto, el alcance para la implantación del SGSI, se debería determinar en primera instancia con el cubrimiento de las áreas de inventario, facturación, contabilidad y entrega de productos, al ser áreas que le permiten de primera mano dar satisfacción a sus clientes. Sin embargo, es imposible dejar de lado otras áreas

[8] SIERRA, LORENA PATRICIA SUAREZ; TARAZONA, CARLOS ALBERTO AMAYA. UNIVERSIDAD NACIONAL ABIERTA YA DISTANCIA ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA. 2013 [En línea]. http://www.usfx.bo/nueva/vicerrectorado/citas/TECNOLOGICAS_20/Informatica/52.pdf

de la empresa, aunque no estén incluidas para el cumplimiento de la misión, pero entran de manera progresiva en el SGSI.[9]

5.9 POLÍTICA DE SEGURIDAD

A continuación se describen todos los aspectos a considerar en el desarrollo de la política de seguridad de la información para una organización, considerando que la política de seguridad es el primer documento que se debe contemplar, por cuanto es donde se especifica toda la normativa interna de la institución con el objetivo de que los funcionarios conozcan y cumplan sobre el sistema de gestión de la seguridad informática (SGSI) establecido, con este documento, también se refleja el compromiso planteado por la dirección. Así mismo contempla todos los aspectos orientados al acceso a la información, utilización de los activos físicos y lógicos de la organización y el comportamiento que debe hacer en caso de que ocurra un incidente de seguridad.

La política de seguridad que se implemente debe demostrar el compromiso de la dirección.

La política de seguridad implementada debe utilizar un lenguaje coherente y claro que lo pueda comprender desde los funcionarios de servicios generales hasta los directivos de la empresa.[10]

[9] Ibíd., SIERRA, y otros.

[10] Ibíd., SIERRA, y otros.

5.10 ANÁLISIS DE REQUISITOS Y DISEÑO DEL SGSI

El análisis de requisitos consiste en estudiar los requerimientos de seguridad de la información para el proceso SGSI bajo la normativa ISO/IEC 27001 definidos. Los requisitos son aquellas exigencias que la normativa determina para el SGSI y son susceptibles de análisis. En tal sentido, la ISO 27003 es la guía que define el análisis de requisitos para direccionar u orientar la implantación de la normativa certificable, definiendo en la cláusula 7 el análisis de requisitos, con los siguientes ítems:

7.2 Definir los requisitos de seguridad de la información para el proceso SGSI

7.3 Identificar los activos dentro de los límites de alcance del SGSI

Procesos / activos clasificación

Activos identificados

7.4 Realizar una evaluación de seguridad de la información[11]

5.11 ESTADO DE SEGURIDAD RESUMIDA DE LA ORGANIZACIÓN

El diseño del SGSI, abarca todos los aspectos de planeación y trazado de la ruta a seguir para la implantación del SGSI en la organización, bajo la normativa en estudio. En consecuencia, la normativa ISO 27003, describe unos aspectos necesarios a considerar en la etapa de diseño en su cláusula 9, los cuales se relacionan a continuación:

[11] Ibíd., SIERRA, y otros.

9.3 Diseño de las TIC y la seguridad de la información física

Plan de ejecución de los controles relacionados con las TIC y la seguridad física

9.4 Control del diseño del SGSI seguridad de la información Específica

9.4.1 Plan de revisiones por la dirección

Lista de insumos para realizar revisión de la gestión
Procedimiento de revisión por la dirección incluye la auditoría, supervisión, aspectos de medición

9.4.2 Formación sobre la seguridad de información de diseño y programa de educación

Materiales de capacitación en seguridad de información

Formación de capacitación en seguridad de información, incluidas las funciones y responsabilidades

Planes de seguridad de la educación sobre la información y la formación

Los registros de educación de seguridad de información y resultados de la formación

9.5 Producir el plan del proyecto SGSI definitiva

Plan de ejecución del proyecto SGSI definitiva[12]

[12] Ibíd., SIERRA, y otros.

5.12 DESARROLLO DE LAS FASES DE IMPLEMENTACIÓN DE UN SGSI

Fase de diagnóstico: Aquí se precisa la situación real de la entidad, identificando adecuadamente los activos de información vinculados a los procesos estratégicos, misionales y de apoyo, así como los riesgos asociados a dichos activos.

Fase de planificación de un SGSI para la organización: Para esta etapa se determinan:

Grupos de trabajo
Establecer mesas de trabajo por cada proceso misional y de apoyo involucrando funcionarios que posean conocimiento de la organización, del área y proceso donde trabajan.

Plan de trabajo
Se determina una metodología en la que se identifique claramente las actividades necesarias, el plazo pertinente para efectuar cada actividad, interrelación entre las mismas y finalmente se designa el personal o equipo para que lleve a cabo cada labor.

Asignación de responsabilidades
La especificación de los límites y compromisos permiten un adecuado monitoreo, por tanto, es importante precisar que se espera de las personas que se asignen al proyecto.

Para el caso en particular se establece:

Tabla 1. Responsables del proyecto

Nombre Responsable	Papel y Función
Ing. Letty Yaneth Moreno Palomeque	Ingeniero de Sistemas-Investigador del proyecto
Ing. Yaciry Enith Palacios Palacios	Ingeniero de Sistemas-Investigador del proyecto
Ing. Daniel Felipe palomo luna	Director Proyecto

Fuente: Autor

Fase de implementación: Acá debe reflejarse el cumplimiento de los objetivos previamente establecidos. Generalmente en esta fase se realiza un comparativo entre lo obtenido Vs lo planificado y así se establece las brechas existentes.

Fase de evaluación y Monitoreo: El objetivo es evaluar los resultados obtenidos una vez fue implementado el SGSI. Esta fase contempla tres tareas a saber:

Evaluación de los resultados del SGSI, diseño del programa de seguimiento, transmitir a los funcionarios el resultado de la evaluación y el mejoramiento continuo del SGSI.

5.13 NIVELES DE MADUREZ DE LOS CONTROLES DE SEGURIDAD

Los niveles de madurez consisten en un conjunto predefinido de áreas de proceso. Los niveles de madurez se miden por el logro de los objetivos genéricos y específicos que se aplican a cada conjunto predefinido de áreas de proceso. En las secciones siguientes se describen las características de cada nivel de madurez en detalle.

Cada nivel de madurez proporciona una capa en la base para una mejora continua del proceso.

Los modelos CMMI (en inglés Capability Maturity Model Integration, Integración de Modelos de Madurez de las Capacidades), con representación por etapas, tienen cinco niveles de madurez designado por los números del 1 al 5. Estos son[13]:

Ilustración 1. Niveles de Madurez

Fuente: https://www.tutorialspoint.com/es/cmmi/cmmi_maturity_levels.htm

5.13.1 Nivel de madurez inicial 1: Los procesos suelen ser ad hoc y caótico. La organización normalmente no proporciona un entorno estable. El éxito de las organizaciones depende de la competencia y de la disposición de las personas de la organización y no en el uso de procesos probados.

Las organizaciones con un nivel de madurez 1 a menudo generan los productos y servicios que funcionan; sin embargo, frecuentemente exceden el presupuesto y el calendario de sus proyectos.

[13] SEI CMMI - Niveles de Madurez. [En línea] https://www.tutorialspoint.com/es/cmmi/cmmi_maturity_levels.htm.

Las organizaciones con un nivel de madurez 1 se caracterizan por una tendencia a abandonar los procesos en el momento de la crisis, y no ser capaz de repetir sus éxitos pasados.[14]

5.13.2 Nivel de madurez 2 administrado: En el nivel de madurez 2, la organización ha logrado todos los objetivos genéricos y específicos de las áreas de procesos. En otras palabras, los proyectos de la organización han asegurado que los requisitos son gestionados y que los procesos se planifican, realizan, medido y controlado.

La disciplina de los procesos reflejados por nivel de madurez 2 ayuda a garantizar que se conserven las prácticas existentes en los momentos de estrés. Cuando estas prácticas están en su lugar, los proyectos se realizan y administran conforme a sus planes documentados correspondientes.

En el nivel de madurez 2, los requisitos, los procesos, los productos de trabajo, y los servicios son administrados. El estado de los productos de trabajo y la prestación de servicios son visibles a la gestión en puntos definidos.

Los compromisos establecidos entre las partes interesadas son revisados en la medida necesaria. Productos de Trabajo son objeto de examen con las partes interesadas y están controlados.

Los productos de trabajo y servicios satisfacen sus requisitos especificados, las normas y objetivos. [15]

---

[14] Ibíd., SEI CMMI

[15] Ibíd., SEI CMMI

5.13.3 Nivel de madurez 3, definida: En el nivel de madurez 3, la organización ha alcanzado todos los objetivos específicos y de las áreas de proceso asignadas a los niveles de madurez 2 y 3.

En el nivel de madurez 3, los procesos están bien caracterizados y entendidos, y se describen en las normas, procedimientos, herramientas y métodos.

Una diferencia fundamental entre el nivel de madurez 2 y el nivel de madurez 3 es el ámbito de los estándares, las descripciones de los procesos y procedimientos. En el nivel de madurez 2, los estándares, las descripciones de los procesos y los procedimientos pueden ser bastante diferentes en cada una de las instancias específicas del proceso (por ejemplo, en un proyecto en particular).

En el nivel de madurez 3, los estándares, las descripciones de los procesos y procedimientos de un proyecto se diseñan a partir del conjunto de procesos estándar de la organización para adaptarse a un determinado proyecto o unidad organizativa. El conjunto de procesos estándar de la organización incluye los procesos abordados en el nivel de madurez 2 y el nivel de madurez 3. Como resultado de ello, los procesos que se llevan a cabo en toda la organización son compatibles excepto por las diferencias de práctica.

Otra diferencia fundamental es que en el nivel de madurez 3, los procesos son normalmente se describe con más detalle y más rigurosa que en el nivel de madurez 2. En el nivel de madurez 3, los procesos son gestionados de manera más proactiva, usando la comprensión de las relaciones de las actividades del proceso y las medidas detalladas del proceso, sus productos de trabajo y sus servicios.[16]

[16] Ibíd., SEI CMMI

5.13.4 Nivel de madurez 4 administrado cuantitativamente: En el nivel de madurez 4, una organización ha logrado todos los objetivos específicos de las áreas de proceso asignadas a los niveles de madurez 2, 3 y 4 y los objetivos genéricos asignados a los niveles de madurez 2 y 3.

En el nivel de madurez 4, se seleccionan los que contribuyen de forma significativa al rendimiento del proceso en general. Estos sub-procesos están controlados mediante técnicas estadísticas y otras técnicas cuantitativas.

Objetivos cuantitativos de calidad y rendimiento de los procesos se establecen y se utilizan como criterios para la gestión de procesos. Los objetivos cuantitativos se basan en las necesidades del cliente, los usuarios finales, la organización, y los responsables de la implementación de los procesos. Calidad y rendimiento de los procesos se entienden en términos estadísticos y se administran a lo largo de la vida de los procesos.

Para estos procesos, las medidas detalladas del rendimiento de los procesos son recogidas y analizadas estadísticamente. Causas Especiales de variación de procesos se identifican y, en su caso, las fuentes de causas especiales están corregidos para evitar que se repita en el futuro.

Calidad y rendimiento de los procesos se hayan incorporado las medidas en la organización del repositorio a medida soporte de toma de decisiones basadas en el futuro.

Una diferencia fundamental entre el nivel de madurez 3 y el nivel de madurez 4 es el grado de previsibilidad del rendimiento de los procesos. En el nivel de madurez 4, el rendimiento de los procesos se controla mediante técnicas estadísticas y otras

técnicas cuantitativas, por lo que es previsible cuantitativamente hablando. En el nivel de madurez 3, los procesos son sólo cualitativamente predecibles.[17]

5.13.5 Nivel de madurez 5 Optimización: En el nivel de madurez 5, una organización ha logrado todos los objetivos del proceso zonas asignadas a los niveles de madurez 2, 3, 4 y 5, y los objetivos genéricos asignados a los niveles de madurez 2 y 3.

Mejorar continuamente los procesos se basa en una comprensión cuantitativa de las causas comunes de variación inherentes a los procesos.

Este nivel se centra en mejora continua del rendimiento de los procesos a través de los aumentos y mejoras tecnológicas innovadoras.

Los objetivos cuantitativos de mejora de procesos para la organización se establecen y se revisan de forma continua a fin de reflejar los cambios objetivos de negocio, y se utilizan como criterios para la administración de la mejora de procesos. Los efectos de las mejoras implementadas en los procesos se miden y evalúan en relación con los objetivos cuantitativos de mejora de procesos. Tanto los procesos definidos como el conjunto de procesos estándar de la organización son objetivos para las actividades de mejora considerables.

Optimización de los procesos ágiles e innovadores, depende de la participación de un personal capacitado y alineado con los valores y objetivos empresariales de la organización. La capacidad de la organización para responder con rapidez a los cambios y oportunidades se mejora mediante la búsqueda de formas para compartir

[17] Ibíd., SEI CMMI

y fomentar el aprendizaje. Mejora de los procesos es, inherentemente, un papel que todo el mundo tiene que jugar, lo que se traduce en un ciclo de mejora continua.

Una diferencia fundamental entre el nivel de madurez 4 y el nivel de madurez 5 es el tipo de variación de procesos. En el nivel de madurez 4, los procesos se encargan de causas especiales de variación de procesos y proporcionan estadísticas para prever los resultados. A pesar de que los procesos pueden producir resultados previsibles, los resultados pueden no ser suficientes para alcanzar los objetivos establecidos. En el nivel de madurez 5, los procesos se encargan de causas comunes de la variación de procesos y el cambio de los procesos (es decir, el cambio del medio de rendimiento del proceso) para mejorar el rendimiento (al mismo tiempo que mantiene estadísticas para prever) para alcanzar los objetivos cuantitativos de mejora de procesos.

5.13.6 Los niveles de madurez no se deben omitir: Cada nivel de madurez proporciona un fundamento necesario para la aplicación efectiva de los procesos en el siguiente nivel:

- Los procesos a un nivel superior tienen menos posibilidades de éxito sin la disciplina de los niveles inferiores.

- El efecto de la innovación puede ser ocultada en un ruidoso proceso.

Un mayor nivel de madurez de procesos puede ser realizado por las organizaciones de menor nivel de madurez, con el riesgo de no ser aplicado de manera consistente en una crisis.[18]

18 Ibíd., SEI CMMI

6 MARCO CONCEPTUAL

Se presentan algunas definiciones importantes relacionadas al SGSI que se busca diseñar.

Políticas de seguridad: Permiten mantener el control de todas las actividades que se realizan en un sistema de información y permite evaluar cada una de las acciones.

Análisis de riesgos: Proceso que permite la identificación, análisis y administración de los riesgos internos y externos que posee una organización.

Sistema de Información: Son procesos que permite almacenar y procesar información; como todo sistema, es el conjunto de partes interrelacionadas: en este caso, hardware, software y recursos humanos. El hardware incluye computadoras o cualquier tipo de dispositivo electrónico, que consisten en procesadores, memoria, sistemas de almacenamiento externo, etc. El software incluye al sistema operativo, firmware y aplicaciones, siendo especialmente importante los sistemas de gestión de bases de datos. Por último, el soporte humano incluye al personal técnico que crean y mantienen el sistema (analistas, programadores, operarios, etc.) y a los usuarios que lo utilizan.

Políticas de seguridad: Busca establecer reglas para proporcionar la dirección gerencial y el soporte para la seguridad de la información. Es la base del SGSI.

Organización de la seguridad de la información: Busca administrar la seguridad dentro de la compañía, así como mantener la seguridad de la infraestructura de procesamiento de la información y de los activos que son accedidos por terceros.

Gestión de activos: Busca proteger los activos de información, controlando el acceso solo a las personas que tienen permiso de acceder a los mismos. Trata de que cuenten con un nivel adecuado de seguridad.

Control de accesos: El objetivo de esta sección es básicamente controlar el acceso a la información, así como el acceso no autorizado a los sistemas de información y computadoras. De igual forma, detecta actividades no autorizadas.

Cumplimiento: Busca que la empresa cumpla estrictamente con las bases legales del país, evitando cualquier incumplimiento de alguna ley civil o penal, alguna obligación reguladora o requerimiento de seguridad. A su vez, asegura la conformidad de los sistemas con políticas de seguridad y estándares de la organización.

Seguridad de la Información: Es la preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.

7 MARCO LEGAL

7.1 NORMAS NACIONAL

7.1.1 Ley 1273 de 2009: 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”.

Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales.

No hay que olvidar que los avances tecnológicos y el empleo de los mismos para apropiarse ilícitamente del patrimonio de terceros a través de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de cómputo para recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas y afectación de los cajeros automáticos, entre otras, son conductas cada vez más usuales en todas partes del mundo.

Esta ley se adiciona al Código Penal colombiano el Título VII BIS denominado "De la Protección de la información y de los datos" que divide en dos capítulos, a saber: “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” y “De los atentados informáticos y otras infracciones”.

El capítulo primero adiciona el siguiente articulado (subrayado fuera del texto):

- Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- Artículo 269B: OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

- Artículo 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

- Artículo 269D: DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- Artículo 269E: USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del

territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- Artículo 269F: VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Al respecto es importante aclarar que la Ley 1266 de 2008 definió el término dato personal como “cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica”. Dicho artículo obliga a las empresas un especial cuidado en el manejo de los datos personales de sus empleados, toda vez que la ley obliga a quien “sustraiga” e “intercepte” dichos datos a pedir autorización al titular de los mismos.

- Artículo 269G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la

creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Es primordial mencionar que este artículo tipifica lo que comúnmente se denomina “phishing”, modalidad de estafa que usualmente utiliza como medio el correo electrónico pero que cada vez con más frecuencia utilizan otros medios de propagación como por ejemplo la mensajería instantánea o las redes sociales. Según la Unidad de Delitos Informáticos de la Policía Judicial (Dijín) con esta modalidad se robaron más de 3.500 millones de pesos de usuarios del sistema financiero en el 2006.

Un punto importante por considerar es que el artículo 269H agrega como circunstancias de agravación punitiva de los tipos penales descritos anteriormente el aumento de la pena de la mitad a las tres cuartas partes si la conducta se cometiere:

Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
Por servidor público en ejercicio de sus funciones

Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

Revelando o dando a conocer el contenido de la información en perjuicio de otro.
Obteniendo provecho para sí o para un tercero.

Con fines terroristas o generando riesgo para la seguridad o defensa nacional.

Utilizando como instrumento a un tercero de buena fe.

Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

Es de anotar que estos tipos penales obligan tanto a empresas como a personas naturales a prestar especial atención al tratamiento de equipos informáticos, así como al tratamiento de los datos personales más teniendo en cuenta la circunstancia de agravación del inciso 3 del artículo 269H que señala “por quien tuviere un vínculo contractual con el poseedor de la información”.

Por su parte, el capítulo segundo establece:

- Artículo 269I: HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 del Código Pena, es decir, penas de prisión de tres (3) a ocho (8) años.
- Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes.

La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

Así mismo, la Ley 1273 agrega como circunstancia de mayor punibilidad en el artículo 58 del Código Penal el hecho de realizar las conductas punibles utilizando medios informáticos, electrónicos o telemáticos.

Como se puede apreciar, la Ley 1273 es un paso importante en la lucha contra los delitos informáticos en Colombia, por lo que es necesario que se esté preparado legalmente para enfrentar los retos que plantea.

7.1.2 Ley 1581 de 2012 Protección de Datos Personales

Generalidades

La ley de protección de datos personales – Ley 1581 de 2012 – es una ley que complementa la regulación vigente para la protección del derecho fundamental que tienen todas las personas naturales a autorizar la información personal que es almacenada en bases de datos o archivos, así como su posterior actualización y rectificación. Esta ley se aplica a las bases de datos o archivos que contengan datos personales de personas naturales.

¿Qué es un dato personal?

Es cualquier información vinculada o que pueda asociarse a una o varias personas naturales que, dependiendo de su grado de utilización y acercamiento con la intimidad de las personas podrá ser pública, semiprivada o privada.

DATO PERSONAL PÚBLICO: Son aquellos datos personales que las normas y la Constitución han determinado expresamente como públicos y, para cuya recolección y tratamiento, no es necesaria la autorización del titular de la información. (Ej. Dirección, teléfono, datos contenidos en sentencias judiciales ejecutoriadas, datos sobre el estado civil de las personas, entre otros.)

DATO PERSONAL SEMIPRIVADO: Son datos que no tienen una naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular, sino a un grupo de personas o a la sociedad en general. Para su tratamiento se requiere la autorización expresa del titular de la información. (Ej. Dato financiero y crediticio).

DATO PERSONAL PRIVADO: Es un dato personal que por su naturaleza íntima o reservada solo interesa a su titular y para su tratamiento requiere de su autorización expresa. (Ej. Nivel de escolaridad)

DATO PERSONAL SENSIBLE: Es aquel dato personal de especial protección, por cuanto afecta la intimidad del titular y su tratamiento puede generar discriminación. NO puede ser objeto de tratamiento a menos que sea requerido para salvaguardar un interés vital del titular o este se encuentre incapacitado y su obtención haya sido autorizada expresamente. (Ej. Origen racial o étnico, orientación política, convicciones religiosas, datos biométricos, relativos a la salud, entre otros.)

8 MARCO CONTEXTUAL

8.1 RESEÑA

UNISANAR IPS Con Nit: 818002.414-2, creada mediante documento privado de comerciante del 26 de marzo del 2004 y registro de cámara de comercio Nº 28622 y Código de prestador de servicio 270010016401 de la Secretaria de Salud Chocó de fecha 24 de junio de 2004 y definida como prestador Privado.

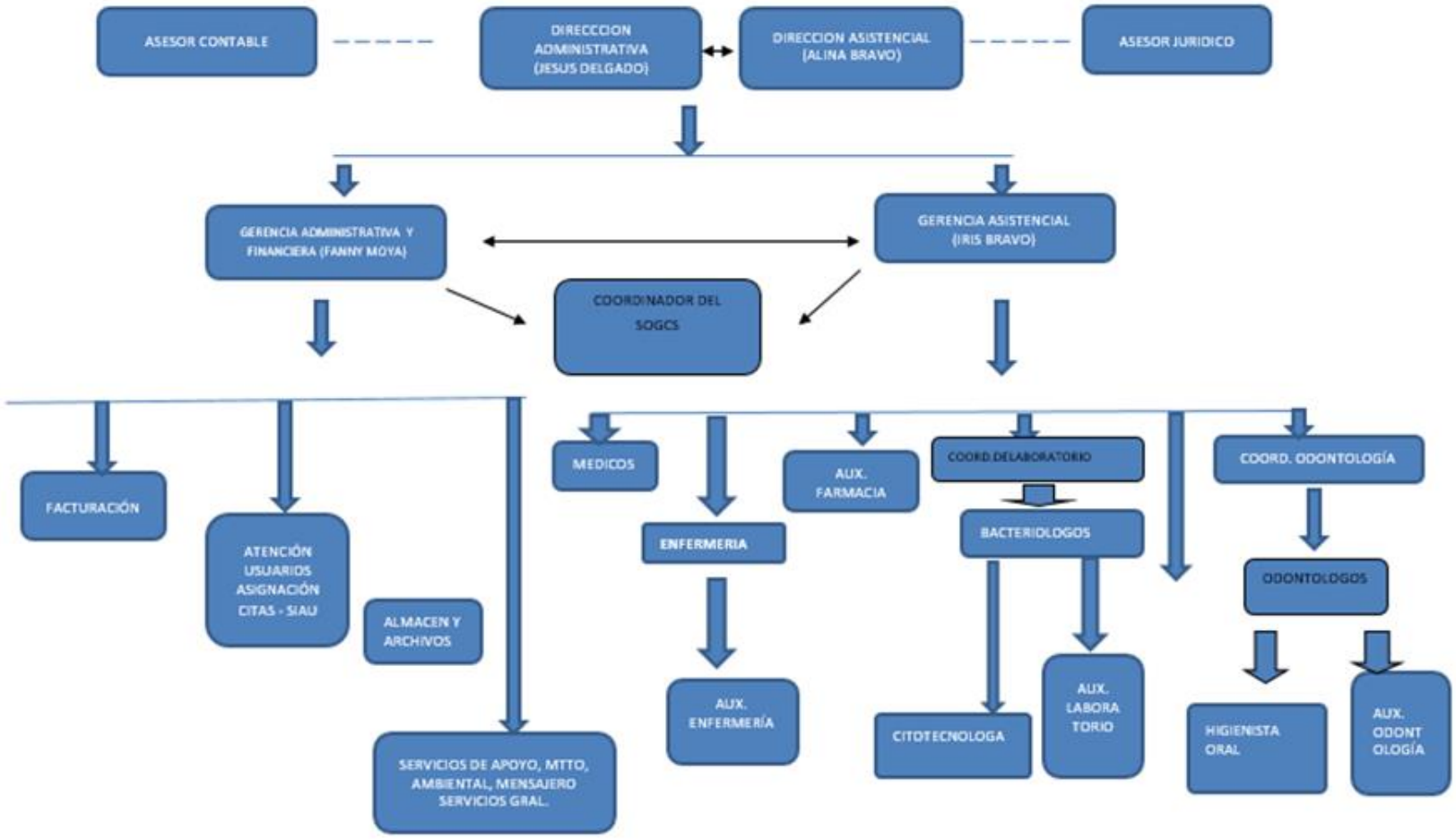
Empresa fundada en el año 2004 como institución prestadora de servicio de salud y con una alternativa diferente en la concepción y modelo en la prestación de servicios de salud en toda la geografía del Chocó, para proporcionar atención a los usuarios en la sede, en su domicilio, en su trabajo lo que representa múltiples ventajas ante la perspectiva de su Institucionalización.

8.2 DIRECCIONAMIENTO ESTRATÉGICO

8.2.1 Misión: Prestar servicios de salud domiciliarios y ambulatorios con calidad, respeto, humanismo, oportunidad, eficiencia, contribuyendo con el mejoramiento de la calidad de vida de la población asistida, conscientes de la confianza generada en el usuario posicionara nuestros servicios como los mejores de la región.

8.2.2 Visión: Ser una Empresa de Salud Pionera en el Departamento del Choco, como Prestadora de Servicios de Salud Domiciliarios y Ambulatorios, con la mejor Calidad, Seguridad y Confiabilidad, Satisfaciendo las Necesidades y Expectativas de los Clientes Internos y Externos, Comprometidos con la Sostenibilidad Financiera y la Perdurabilidad.

Ilustración 2. Estructura orgánica de UNISANAR IPS



Fuente: Proporcionada por la Gerencia de UNISANAR IPS

9 METODOLOGÍA DE DESARROLLO DEL PROYECTO

Esta monografía se desarrollará realizando las siguientes fases:

Ilustración 3. Metodología Para Desarrollar

Fuente: Autor

9.1 FASES DEL PROYECTO

Esta monografía pretende desarrollar las siguientes fases

Fase I: Recopilar información pertinente de las áreas, con el propósito de identificar problemas y oportunidades de mejora, mediante observaciones y encuestas.

Fase II: Analizar la información recopilada para identificar los riesgos, evaluarlos y proponer los controles de seguridad que los mitiguen.

Fase III: Diseño de la propuesta de políticas y controles para el sistema de seguridad de información.

9.2 LEVANTAMIENTO DE INFORMACIÓN

Inicialmente se realiza el levantamiento de información que es la etapa inicial más importante donde se establecen los parámetros necesarios para entender y modelar completamente el sistema de una forma dinámica.

9.3 TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

En aras de obtener buenos resultados se empleará como técnica e instrumento de recolección de información la investigación cualitativa y cuantitativa; mediante el seguimiento y observación de los espacios, entrevistas informales de conocimiento y encuestas dirigidas a los empleados en general y en especial al grupo de facturación encargados en la actualidad de gestionar el software de almacenamiento de información de los usuarios. Esto con el fin de poder obtener unos resultados más precisos en cuanto a la situación de vulnerabilidad que atraviesa la empresa UNISANAR IPS.

9.3.1 Fuentes primarias. Mediante las encuestas podremos analizar de forma clara e identificar cada una de las situaciones que producen la vulnerabilidad y conseguir estrategias para dar soluciones optimas a la situación, como es la implementación de la norma ISO/IEC 27001, que ayudara a obtener la certificación partiendo de los datos de la organización y la implantación del SGSI de acuerdo con la necesidad de la empresa UNISANAR IPS.

9.3.2 Fuentes secundarias: Se harán consultas relacionadas con la investigación en materiales multimedia, libros, páginas web, con el fin que sirvan como herramienta y apoyo a la solución de cada uno de los objetivos.

9.4 TIPO DE ANÁLISIS

Es importante, tener como ayudas la parte numérica como gráfica, por lo que se hace primordial trabajar con la técnica cualitativa y cuantitativa, esto permite de una manera más didáctica el entendimiento para la toma de decisión.

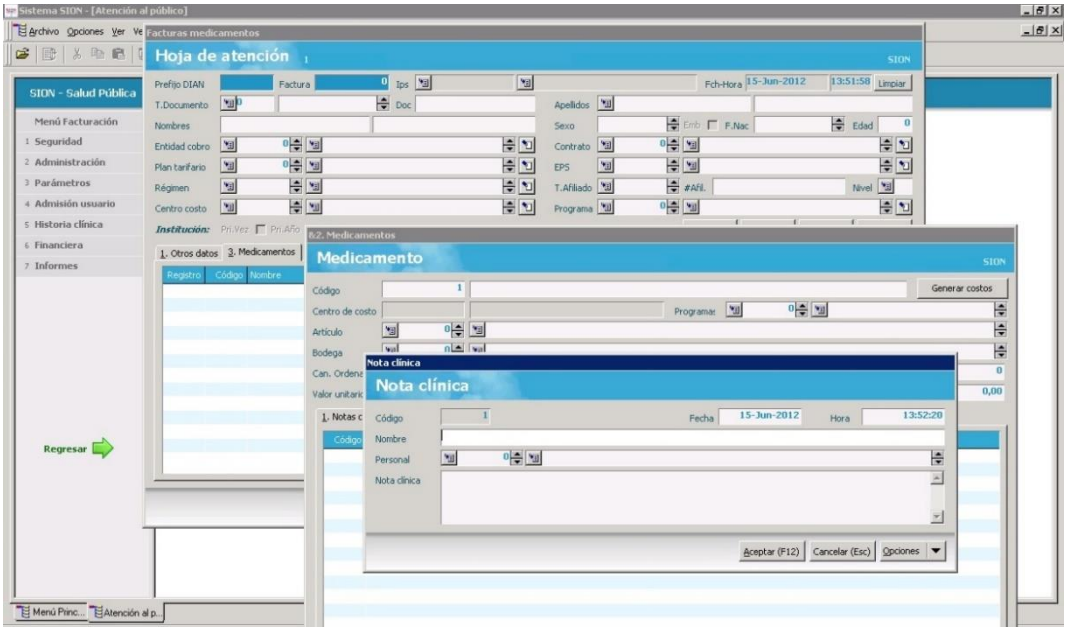
10 DESARROLLO DEL PROYECTO

10.1 LEVANTAMIENTO DE LA INFORMACIÓN

El levantamiento de la información requerida, se efectuó mediante una visita a la entidad, verificando con el método de observación inicialmente, se revisó cada una de sus dependencias y mediante entrevistas verbales con algunos empleados sobre el manejo de la mismas, y tenían unas cámaras de seguridad pero al hacer el traslado de la empresa por arreglos internos no las volvieron a instalar, aparte de eso contaban con un digiturno pero manifiesta el gerente que lo tienen archivado hasta que se instalen nuevamente en las instalaciones propias las cuales se demoran ya que están en proceso de remodelación desde hace tres años y es por ello, el poco interés de tener instalaciones de seguridad en los lugares donde se han trasladado por diferentes razones.

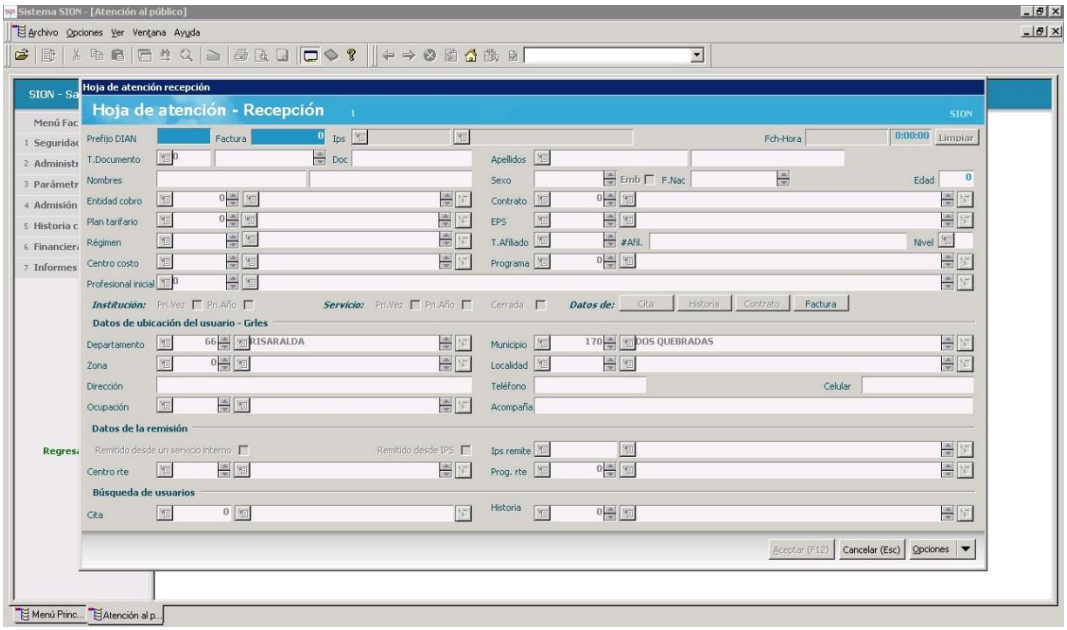
Se entablo comunicación presencial con la encargada de facturación quien manifestó que manejan un software llamado INFOSALUD, el cual está dividido por módulos donde es necesario un usuario y contraseña para cada uno de los mismos; en la actualidad la IPS UNISANAR, trabaja con los módulos de cita, historia clínicas, facturación, procesos, formulario de: medicamento, recepción, orden médica; aunque existen otros módulos como el KARDEX, farmacia, tablas, no son empleadas toda vez que en la actualidad no las requieren. Este software es actualizado por los creadores mediante la carpeta FACTUP, donde le anexan las últimas normas y todo lo requerido por su usuario. Cabe resaltar que la encargada o administradora local de este sistema, hace copia de seguridad diaria, almacenando la información en la nube de Dropbox, en memorias, o diferentes equipos, con el fin de evitar perder toda la información que hasta la fecha llevan.

Ilustración 4. Formulario de medicamentos



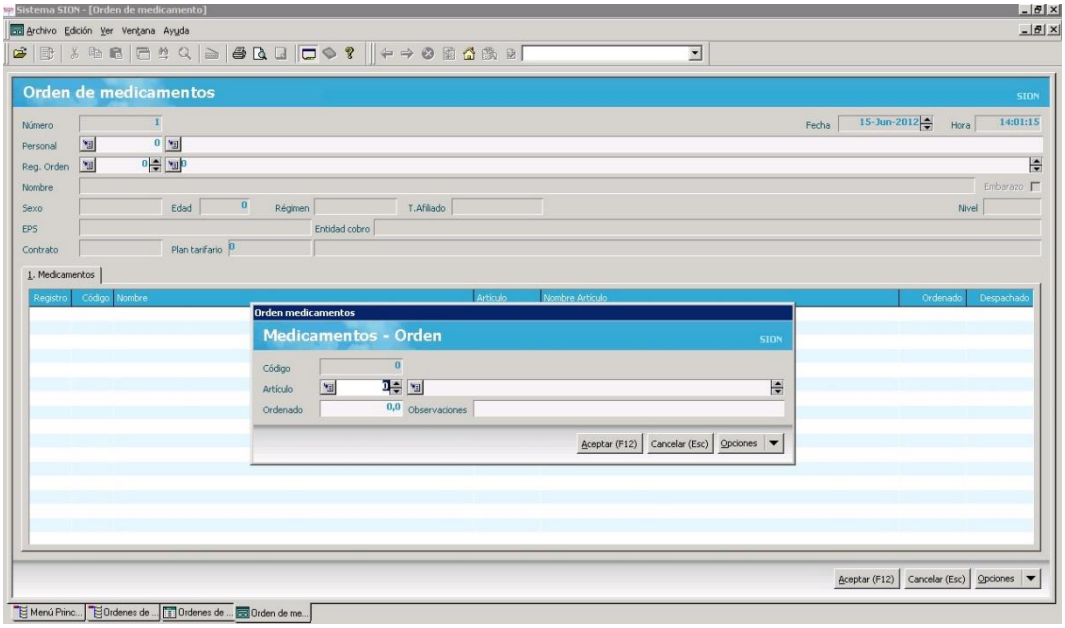
Fuente: El autor

Ilustración 5. Recepción



Fuente: El autor

Ilustración 6. Orden de medicamento



Fuente: El autor

En cuanto a la parte de sistemas, inicialmente contaban con un pequeño switch para 15 puertos, de los cuales solo tenían conectados 6 equipos, uno de ellos funciona como servidor y es donde siempre han tenido instalado el INFOSALUD, pero sin seguridad, pues es el equipo que maneja la funcionaria del área de facturación.

Tiene una página www.unisanar.com, la cual le pagan el dominio, pero nunca la han utilizado al igual que los correos empresariales, aparte que aún sigue en proceso de construcción.

Ilustración 7. Página UNISANAR

Fuente: El autor

Como se puede visualizar en la imagen, la página de la entidad se encuentra en reparación, es de anotar que está no se ha utilizado por la falta de información al día y aún continúan almacenando los datos de manera física.

En la actualidad se encuentran en una casa de alquiler donde adecuaron la oficina, la cual cuenta con 200 funcionarios, tienen 15 equipos con internet WIFI, 17 equipos por cableado, tienen 5 líneas telefónicas, 11 impresoras, 3 escáneres y muchos equipos son portátiles personales.

10.1.1 Entrevista con el personal: Resultados de las entrevistas a los funcionarios de proceso misionales y de apoyo para establecer la existencia de una política y procedimientos de seguridad.

Una vez socializado el fin de esta entrevista a los funcionarios de UNISANAR IPS, se procedió a su aplicación y tabulación de los resultados obteniendo lo siguiente:

Tabulación - Seguridad en General

1. ¿De cuántos ordenadores dispone UNISANAR IPS?

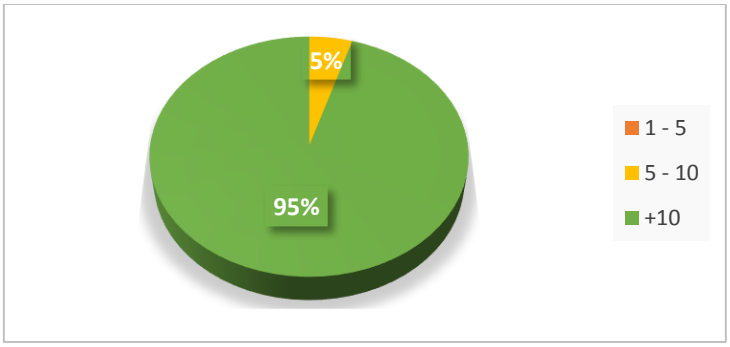
1-5 5-10 +10

Tabla 2. Tabulación respuestas pregunta No.1

Valor ponderado	Frecuencia	Porcentaje %
1-5	0	0%
5-10	1	5%
+10	20	95%
Total	21	100%

Fuente: El autor

Ilustración 8. Cantidad de equipos de cómputo



Fuente: El autor

Dado que UNISANAR IPS no tienen el mismo número de funcionarios se aprecia que la mayor parte de los procesos cuenta con más de 10 computadores representando el 95% y la dependencia que posee menos equipos entre 5 a 10 corresponde al 5%.

2. Los equipos de cómputo de la entidad, ¿tienen instalado antivirus?

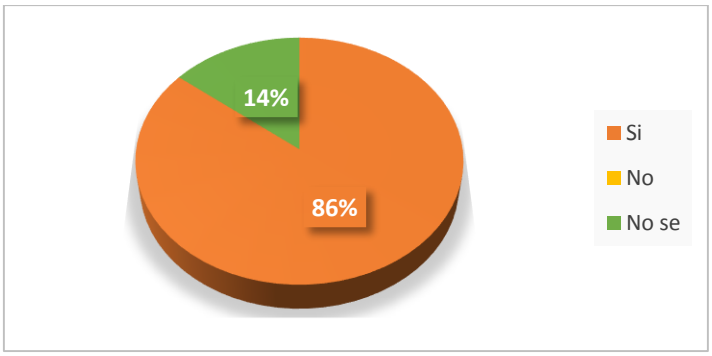
Sí No No se

Tabla 3. Tabulación respuestas pregunta No. 2

Valor ponderado	Frecuencia	Porcentaje %
Si	18	86%
No	0	0%
No se	3	14%
Total	21	100%

Fuente: El autor

Ilustración 9. Existencia de Antivirus



Fuente: El autor

A partir de los datos obtenidos en la encuesta se observa que el 86% de los empleados tienen instalado un antivirus como medida de protección contra amenazas de un virus que pueda afectar el normal funcionamiento del equipo y un 14% no tiene conocimiento al respecto.

3. El antivirus que tienen instalado (si es el caso), ¿está actualizado con las últimas definiciones?

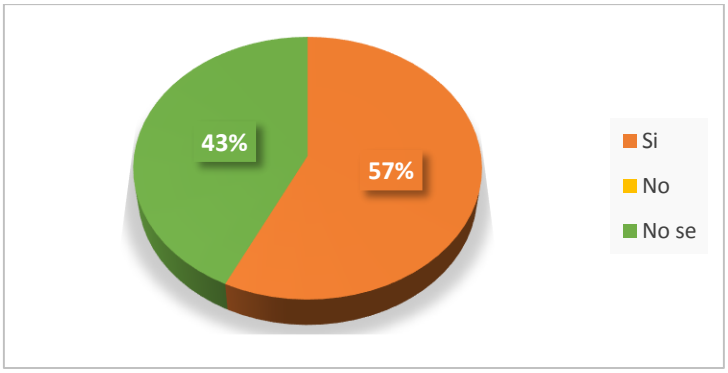
Sí No No se

Tabla 4. Tabulación respuestas pregunta No. 3

Valor ponderado	Frecuencia	Porcentaje %
Si	12	57%
No	0	0%
No se	9	43%
Total	21	100%

Fuente: El autor

Ilustración 10. Actualización de Antivirus



Fuente: El autor

Una vez formulada las dos preguntas enunciadas con anterioridad a los entrevistados, se evidencia que el 57% respondieron afirmativamente que el antivirus está actualizado de acuerdo con las últimas definiciones.

Tan solo un 43% manifestó no saber si este era actualizado de acuerdo con los requerimientos establecidos.

4. ¿Se realiza un mantenimiento informático periódico sobre los ordenadores de la empresa?

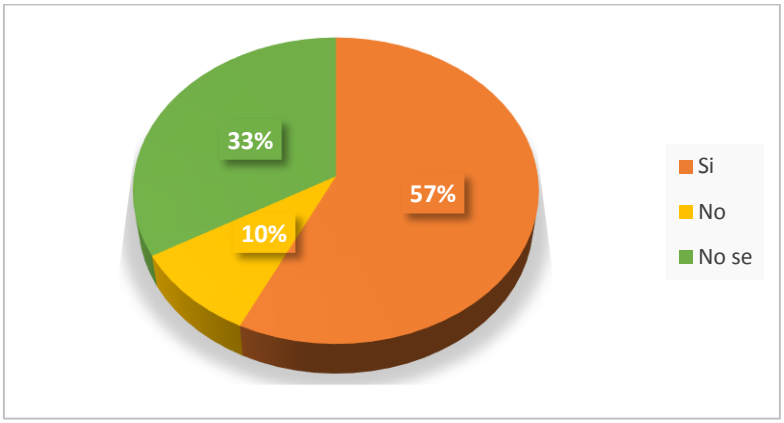
Sí No No se

Tabla 5. Tabulación respuestas pregunta No. 4

Valor ponderado	Frecuencia	Porcentaje %
Si	12	57%
No	2	10%
No se	7	33%
Total	21	100%

Fuente: El autor

Ilustración 11. Mantenimiento preventivo



Fuente: El autor

El 57% de la población entrevistada afirmo que en UNISANR IPS se realiza cada 6 meses el mantenimiento preventivo a los equipos de cómputo, esto de acuerdo con un cronograma previamente definido y aceptado por los directivos y un 33% manifiestan no tener conocimiento al respecto. Dicho mantenimiento toma aproximadamente 1 hora por equipo.

5. ¿Se utilizan programas de descarga de archivos de usuario (música, películas, programas...)?

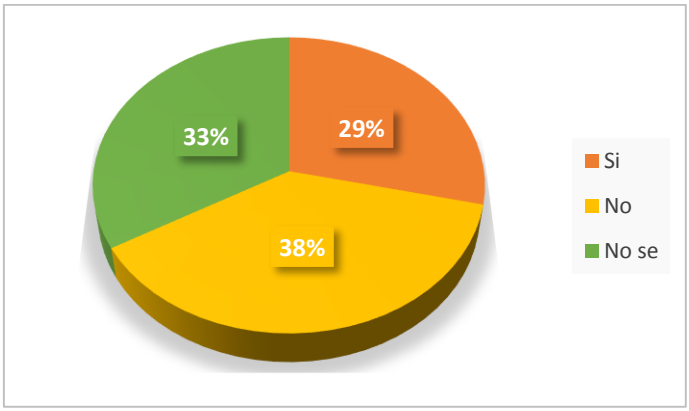
Sí No No se

Tabla 6. Tabulación respuestas pregunta No. 5

Valor ponderado	Frecuencia	Porcentaje %
Si	6	29%
No	8	38%
No se	7	33%
Total	21	100%

Fuente: El autor

Ilustración 12. Programas de descarga libre



Fuente: El autor

En este caso, el 38% indicó que no era posible instalar programas que no fueran autorizados por la oficina de sistemas. Por su parte, el 29% declararon que si se hace uso de aplicaciones de uso gratuito para descargar no solo música sino otro tipo de archivos multimedia a pesar de que se esté incurriendo en el incumplimiento de la "CARTA DE COMPROMISO DE LICENCIAMIENTO, USO DE SOFTWARE Y CUMPLIMIENTO DE POLÍTICAS INFORMÁTICAS", en tanto a las personas que indicaron no saber si este tipo de descargas se estaban efectuando al interior del área, coincidieron en que no era posible hacerlo dado que estaba prohibido en UNISANAR IPS.

6. ¿Conoce si UNISANAR IPS cuenta con un servidor central de datos?

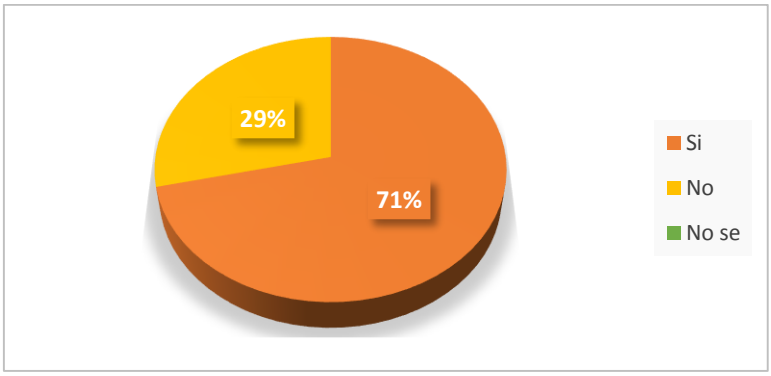
Sí No No se

Tabla 7. Tabulación respuestas pregunta No. 6

Valor ponderado	Frecuencia	Porcentaje %
Si	15	71%
No	6	29%
No se	0	0%
Total	21	100%

Fuente: El autor

Ilustración 13. Servidor central



Fuente: El autor

Como se puede apreciar en el gráfico el 71% de los empleados tienen noción de que en la entidad se cuenta con un servidor central de datos y un 29% no sabe la existencia de un servidor.

7. Sobre dicho servidor, ¿sabe si se le realiza un mantenimiento informático periódico?

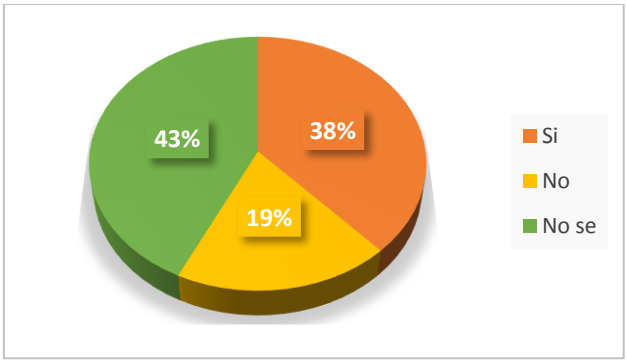
Sí No No se

Tabla 8. Tabulación respuestas pregunta No. 7

Valor ponderado	Frecuencia	Porcentaje %
Si	8	38%
No	4	19%
No se	9	43%
Total	21	100.00%

Fuente: El autor

Ilustración 14. Mantenimiento informático



Fuente: El autor

Para este cuestionamiento las respuestas no coincidieron en cuanto a saber si existía o no un servidor central de datos puesto que un 43% asumieron no saber nada del mantenimiento de un servidor central debido a que no conocen la existencia del mismo y un 38% afirman que si se realiza mantenimiento informático periódico al servidor central de datos. Es de notar que hay desconocimiento en cuanto a los activos informáticos y su manejo.

8. ¿En la entidad se trabaja desde algún ordenador externo, por conexión vía Internet?

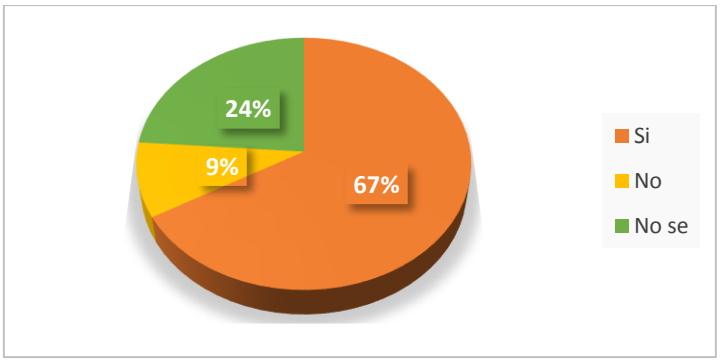
   Sí No No se

Tabla 9. Tabulación respuestas pregunta No. 8

Valor ponderado	Frecuencia	Porcentaje %
Si	14	67%
No	2	9%
No se	5	24%
Total	21	100%

Fuente: El autor

Ilustración 15. Conexión



Fuente: El autor

Con un 67% la respuesta SI tiene la mayor representación; es por esto que se evidencia que hay conocimiento por parte de los funcionarios de proceso, en UNISANAR IPS, tan solo el 24% de los entrevistados respondió no saber que se gestionan procesos desde fuera de las instalaciones.

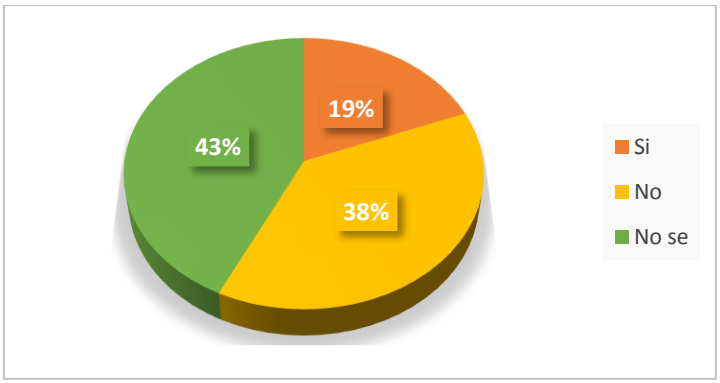
9. Si la conexión en UNISANAR IPS es mediante la red (WIFI), ¿conoce si se utilizan las medidas de seguridad pertinentes para proteger dicha conexión?
   Sí No No se

Tabla 10. Tabulación respuestas pregunta No. 9

Valor ponderado	Frecuencia	Porcentaje %
Si	4	19%
No	8	38%
No se	9	43%
Total	21	100%

Fuente: El autor

Ilustración 16. Medidas de seguridad



Fuente: El autor

En este aspecto, se puede observar que el 43% desconocen el hecho de haber conexión de esta forma y, sin embargo, el 38% informa que no tienen conexión WI-FI y por su parte el 19% indica que sí tiene conexión WI-FI en UNISANAR IPS y que cuenta con las medidas pertinentes.

10. ¿Los computadores de la entidad tienen datos de la empresa almacenados en el disco duro?

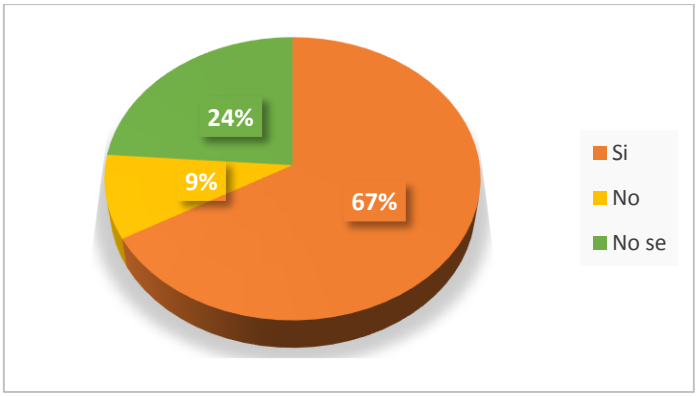
Sí No No se

Tabla 11. Tabulación respuestas pregunta No. 10

Valor ponderado	Frecuencia	Porcentaje %
Si	14	67%
No	2	9%
No se	5	24%
Total	21	100%

Fuente: El autor

Ilustración 17. Almacenamiento de Disco Duro



Fuente: El autor

En base a la encuesta y cómo podemos observar en el gráfico, el 67% de los entrevistados afirmaron que efectivamente la mayoría de la información de la entidad reposa en cada una de las estaciones de trabajo por seguridad. Por otro lado un 24% desconocen la realización de copias de seguridad de la información almacenada.

11. ¿Se realiza copia de seguridad de la información que maneja la entidad?

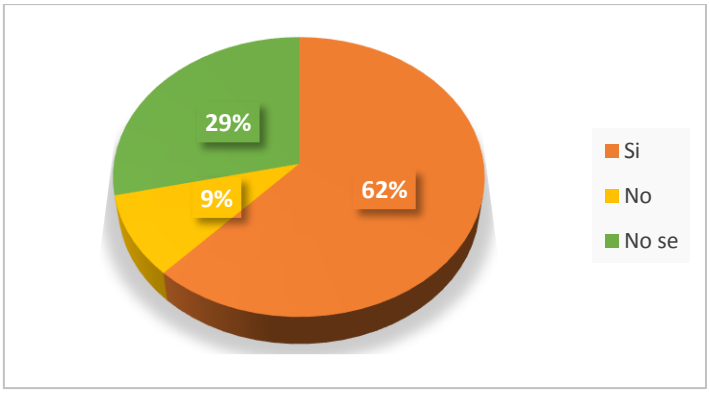
Sí No No se

Tabla 12. Tabulación respuestas pregunta No. 11

Valor ponderado	Frecuencia	Porcentaje %
Si	13	62%
No	2	9%
No se	6	29%
Total	21	100%

Fuente: El autor

Ilustración 18. Copia de seguridad



Fuente: El autor

12. ¿Con qué frecuencia?

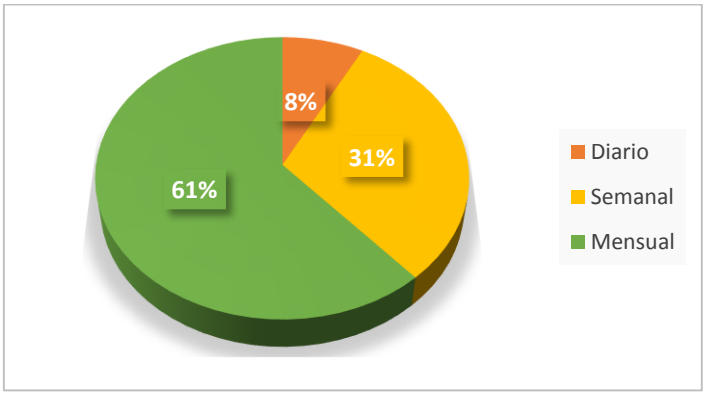
Diaria semanal otro

Tabla 13. Tabulación respuestas pregunta No. 12

Valor ponderado	Frecuencia	Porcentaje %
Diario	1	8%
Semanal	4	31%
Mensual	8	61%
Total	21	100%

Fuente: El autor

Ilustración 19. Frecuencia Copia de seguridad



Fuente: El autor

El 62% de los entrevistados coincidieron en que se realizan copias de seguridad con el fin de respaldar la disponibilidad de la información, esta práctica esta apropiada por los funcionarios más por ser una exigencia que por el sentido mismo de su importancia a la hora de mantener la información dispuesta cuando esta se requiera y un 29% no sabe realizar dicho proceso. En tanto a la frecuencia con la que se realizan las copias de seguridad el 61% indica que esta se realiza mensualmente debido a la importancia de la información, el 31% indica que lo hace semanalmente debido a la sensibilidad de los datos manejados por la entidad y por su parte solo el 8% responde que estas se llevan a cabo diariamente según sea la necesidad.

13. ¿Usted o sus colaboradores a cargo poseen alguna copia de seguridad (USB / DVD / Otro) fuera de la empresa?

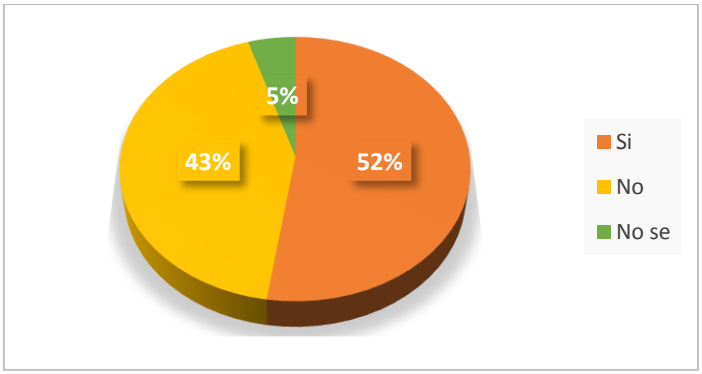
    Sí No No se

Tabla 14. Tabulación respuestas pregunta No. 13

Valor ponderado	Frecuencia	Porcentaje %
Si	11	52%
No	9	43%
No se	1	5%
Total	21	100%

Fuente: El autor

Ilustración 20. Existe Copia de seguridad



Fuente: El autor

El 52% revela que realizan copias de seguridad en dispositivos extraíbles por su tranquilidad debido a que no tienen la certeza de que la información haya sido guardada. El 43% revela que no es posible guardar copias de seguridad en dispositivos extraíbles, esto a raiz que no cuentan con dichos dispositivos. El restante 5% aclaró desconocimiento del tema en cuestión.

14. ¿Se realiza un mantenimiento de las copias de seguridad de UNISANAR IPS?

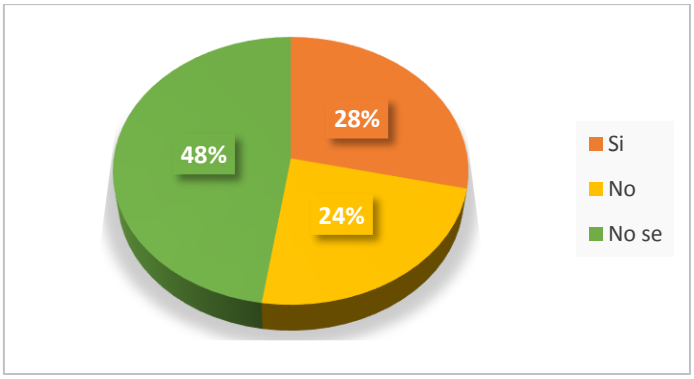
Sí No No se

Tabla 15. Tabulación respuestas pregunta No. 14

Valor ponderado	Frecuencia	Porcentaje %
Si	6	28%
No	5	24%
No se	10	48%
Total	21	100%

Fuente: El autor

Ilustración 21. Mantenimiento Copia de seguridad



Fuente: El autor

Se aprecia que en este sentido el 48% de los entrevistados desconocen los procesos que se realizan a las copias de seguridad de UNISANAR, para el 28% de los interrogados afirman tener conocimiento de los mantenimientos que se realiza a la copia de seguridad de la entidad y un 24% responde que no se le realiza este proceso a las copias de seguridad.

15. ¿Los programas y aplicaciones usadas en UNISANAR IPS, cumplen con las características de seguridad informática?

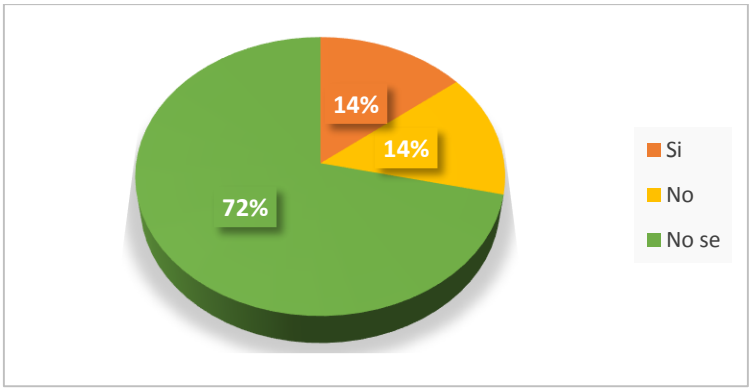
    Sí No No se

Tabla 16. Tabulación respuestas pregunta No. 15

Valor ponderado	Frecuencia	Porcentaje %
Si	3	14%
No	3	14%
No se	15	72%
Total	21	100%

Fuente: El autor

Ilustración 22. Programas y aplicaciones



Fuente: El autor

El 72% no tener conocimiento de la seguridad informática y si las aplicaciones y programas lo aplican, Solo tres funcionarios que equivale al 14% afirman que los sistemas de información cuentan con parámetros de seguridad que garantizan la confiabilidad, integridad y disponibilidad de la información, aunque en si UNISANAR IPS no tiene políticas claramente definidas en materia de software y un 14% niegan que las aplicaciones y programas cuente con los parámetros que requiere de acuerdo a la seguridad informática.

16. ¿Hay algún encargado de instalar/desinstalar los programas y aplicaciones informáticas en UNISANAR IPS?

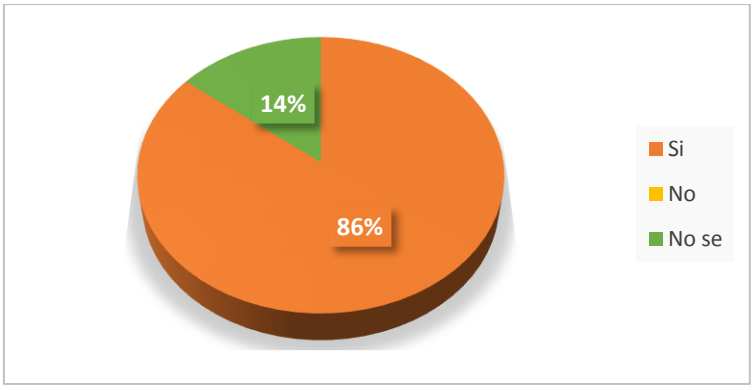
Sí No No se

Tabla 17. Tabulación respuestas pregunta No. 16

Valor ponderado	Frecuencia	Porcentaje %
Si	18	86%
No	0	0%
No se	3	14%
Total	21	100%

Fuente: El autor

Ilustración 23. Instalación/Desinstalación programas



Fuente: El autor

Es claro que la entidad cuenta con una firma externa encargada de realizar las configuraciones pertinentes de acuerdo con la necesidad del proceso que se gestiona. El 86% de los entrevistados afirma conocer que los encargados de esta labor es la secretaría de salud nacional. Un 14% manifiestan no saber quién es el encargado de dicho proceso.

17. ¿Conoce usted algo referente a la seguridad informática?

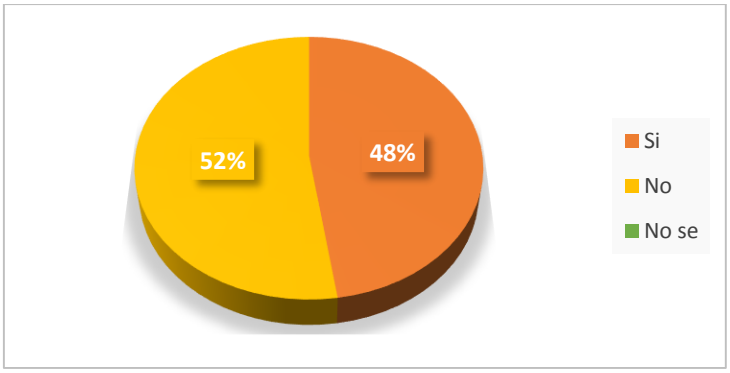
Sí No No se

Tabla 18. Tabulación respuestas pregunta No. 17

Valor ponderado	Frecuencia	Porcentaje %
Si	10	48%
No	11	52%
No se	0	0%
Total	21	100%

Fuente: El autor

Ilustración 24. Concepto seguridad informática



Fuente: El autor

Siendo la seguridad un factor muy importante en el manejo de información en las entidades, es indudable que el desconocimiento es un ingrediente muy común en las organizaciones, como se puede notar el 52% no tienen idea de lo que es la seguridad informática y un 48% afirman saber algo de seguridad informática debido a sus experiencias en otras entidades o por su formación académica.

18. ¿Qué sabe al respecto?

Sobre su conocimiento de la seguridad informática los encuestados respondieron:
La seguridad informática es muy esencial para los datos manejados en la entidad
Es con lo que se protege la información que manipulamos diariamente
Es la protección que cada uno debemos de darle a la información que manipulamos

La verdad no mucho, pero hay una persona en la entidad que se encarga de revisar los equipos y está construyendo una página.
Es el manejo adecuado que le damos a la información
Proceso mediante el cual se protege toda la información que tiene que ver por vía de redes de datos
Es la seguridad que debe tener la empresa evitando ataques
Es la seguridad que todos debemos tener para evitar la pérdida de la información
Es la protección que se brinca a los equipos

19. ¿La compañía ha dispuesto políticas de seguridad para el manejo de las herramientas informáticas de las que disponen para la gestión de su proceso?

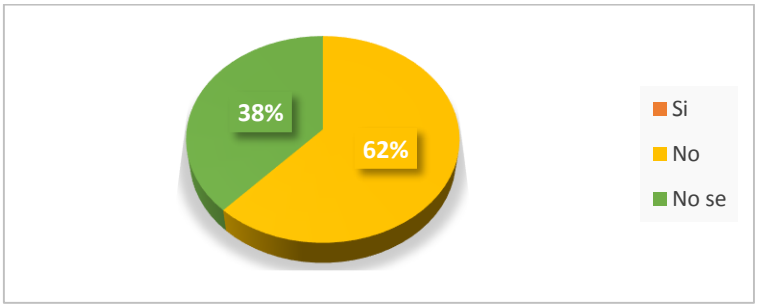
Sí No No se

Tabla 19.Tabulación respuestas pregunta No. 19

Valor ponderado	Frecuencia	Porcentaje %
Si	0	0%
No	13	62%
No se	8	38 %
Total	21	100%

Fuente: El autor

Ilustración 25. Políticas de seguridad



Fuente: El autor

Como se puede observar en la gráfica el 62% niegan el hecho de que en la entidad haya políticas de seguridad en el manejo de la información que dispone cada uno de los procesos de UNISANAR IPS, y un 38% desconocen por completo este tema.

- ¿Cuáles?

La “CARTA DE COMPROMISO DE LICENCIAMIENTO, USO DE SOFTWARE Y CUMPLIMIENTO DE POLÍTICAS INFORMÁTICAS”, algunas disposiciones sobre el uso e instalaciones de software gratuito en los ordenadores de UNISANAR IPS, uso adecuado del correo corporativo y realizar copias de seguridad de acuerdo con la necesidad y vida útil de la información.

20. ¿Qué medidas de seguridad toma para proteger la información de UNISANAR IPS?

En este punto se manifestó:
Realizo copia de seguridad en OneDrive
Hago copia de seguridad en mi USB
Yo tengo un disco duro donde hago la copia de seguridad de mi información solamente
Guardo en mi memoria información
Hago copia de respaldo en disco duro
Backup en USB
No sabe, no responde

Una vez culminada la tabulación y análisis de las entrevistas, se concluye que en UNISANAR IPS se toman algunas medidas de seguridad informática, con el fin de garantizar los activos más valiosos para la entidad, sin embargo, no se ve indicios de establecer un SGSI formal y documentado, razón por la cual el presente proyecto

pretende proponer un SGSI acorde a las necesidades de la entidad y el cual será complementado con los diferentes procedimientos, manuales y directrices ya establecidas a fin de consolidar dicho sistema y que finalmente este sea auditado y certificado por el ente definido para este fin.

10.1.2 Levantamientos activos de la información: Se realizó el levantamiento del inventario de activos de información existentes en UNISANAR IPS, como se relaciona en la siguiente tabla:

Tabla 20. Inventario de activos UNISANAR IPS

TIPO DE ACTIVO	NOMBRE DE ACTIVO UNISANAR
Activo de información	Información de las EPS, afiliados, proveedores y empleados en bases de datos.
Software y Aplicaciones	Sistema operativo Windows XP (5)
	Sistema operativo Windows 7 (26)
	Sistema operativo Windows 8 (5)
	Sistema operativo Windows server (1)
	Office 2007 (32)
	Office 2013 (5)
	Antivirus Kaspersky Licencia 1 año
	Aplicaciones: INFOSALUD
Hardware	32 equipos de cómputo de escritorio
	5 portátiles
	11 impresoras HP LaserJet Enterprise
	3 escáner HP
Servicios	Conectividad a internet (cable, WI-FI)
Personal	179 funcionarios operativos
	14 funcionarios de alta dirección
	7 funcionarios de Vigilancia

Fuente: El autor

Por último, la entidad tiene sucursales en varios municipios del departamento del Chocó, en la sede principal que se encuentra en el municipio de Quibdó cuenta con 14 funcionarios y los otros están en diferentes municipios; los cuales no tienen acceso a internet, lo que genera que la información que reposa en ellos siempre será manual donde estos manifiestan que no harían una inversión tan grande para las zonas rurales en contratos que solo son por periodos electorales.

10.1.2.1 Observación del manejo de la información sensible de la entidad. Como se ha mencionado en anteriores secciones de esta investigación, la entidad no cuenta con políticas de seguridad que garanticen el adecuado manejo de la información sensible y confidencial para la IPS y no solo es una directriz que guie tal manejo sino, además, que el personal no es consciente de que es necesario cultivar la cultura de protección y buen uso de la información. Durante un día normal de trabajo se procedió a visitar la Gerencia, Operaciones cita, facturación, Afiliaciones y novedades; en donde se pudo observar que en la gran mayoría de los casos los procesos se gestionan de forma manual a pesar de contar con sistemas de información; algunas prácticas no son muy seguras y la falta de concientización en materia de seguridad de la información en los documentos, carpetas y otros medios de almacenamiento que contienen información sensible, no están ubicadas en un área protegida, por el contrario, la mayor parte de la información está al alcance de cualquier persona que pueda ingresar a estas áreas.

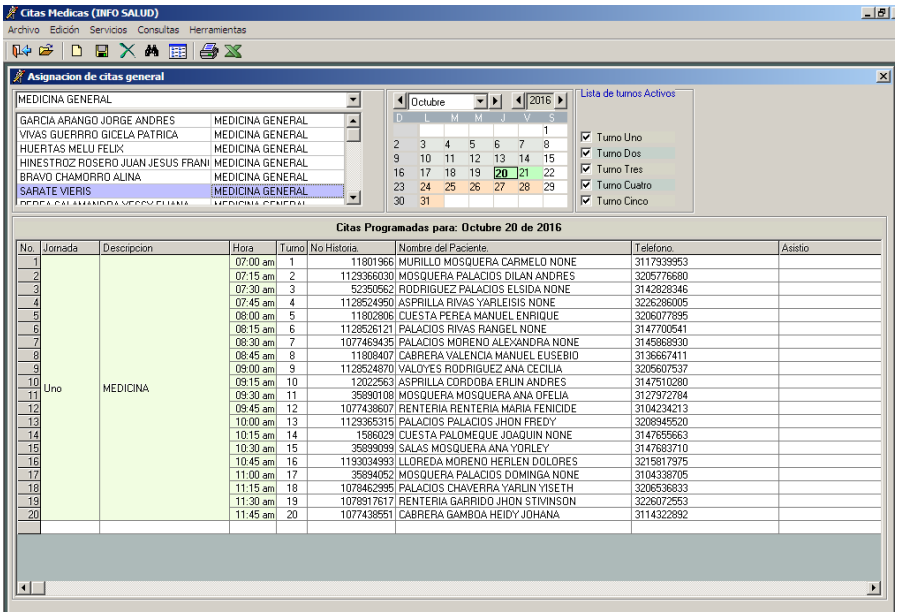
Se observó que muchos de los funcionarios cuando deben retirarse de su lugar de trabajo no bloqueaban el equipo dejando a disposición de cualquiera su estación y la información que en ese momento estaba tratando.

Algunos usuarios apuntan sus contraseñas de ingreso a su computador y aplicaciones en la agenda de trabajo o en memos que dejan sobre su escritorio.

Los computadores portátiles no están asegurados mediante una guaya de seguridad, por lo tanto, están expuestos a que su equipo sea sustraído de forma no autorizada de las instalaciones.

Por su parte la cita se está gestionando de forma manual y a su vez se están registrando en una base de Excel que no tiene ningún respaldo y a la fecha el backup de esta se encuentra en una memoria USB que es utilizada por más de un funcionario.

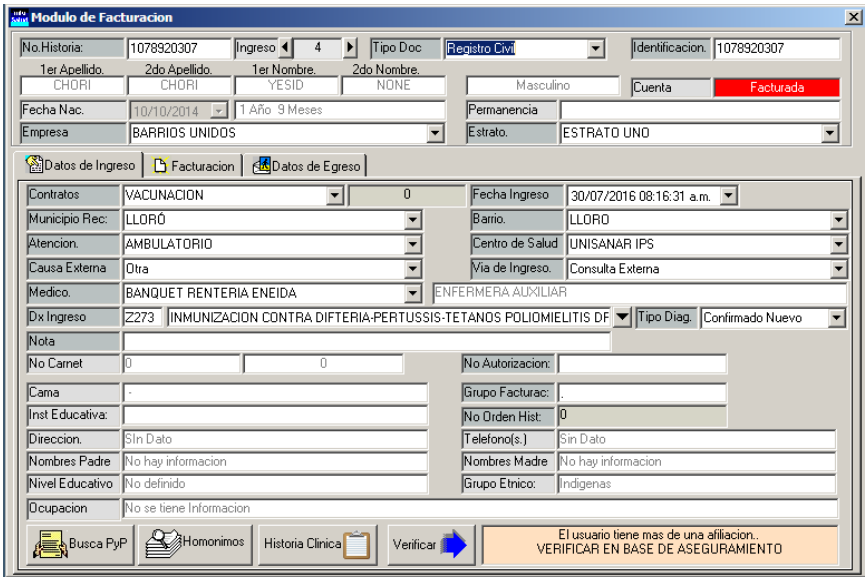
Ilustración 26. Programa de Citas



Fuente: El autor

El registro de los nuevos afiliados o renovación de afiliaciones es tratado por un único funcionario que lo realiza manualmente a través de un archivo de Excel enviado a través de correo electrónico al proveedor encargado de la carga de estos datos sin ninguna medida de seguridad.

Ilustración 27. Programa de Facturación



Fuente: El autor

Es posible que muchas de estas acciones se mejoren sensibilizando a las personas sobre la importancia que tiene respaldar la confidencialidad, integridad y disponibilidad de la información con la cual está comprometida la organización; además, de la estructuración de un SGSI, definición y socialización de políticas de seguridad que permitan garantizar que toda la información es manejada bajo buenas prácticas.

Una vez culminado el análisis y evidenciado las diferentes situaciones que afectan a UNISANAR IPS se estableció que el problema de seguridad está asociado a la falta de un Sistema de Gestión de Seguridad de la Información. Igualmente, a la poca concientización, apropiación y conocimiento en materia de seguridad por parte de los funcionarios, no se dan los espacios necesarios para una participación activa de todos los empleados en la definición de controles de seguridad basados un análisis y evaluación de riesgos.

Por otro lado, se apreció que no hay una diferenciación clara entre seguridad informática y de la información, por parte de los profesionales del área de Sistemas, y por supuesto, los funcionarios del común tampoco pueden diferir entre un término y otro; además no se cuenta con un sistema apropiado para la gestión y valoración de riesgos de seguridad y por último no se tiene una política de seguridad establecida y que esta esté alineada con la plataforma estratégica del oficio.

10.1.2.2 *Análisis de la situación actual y recomendación de aplicabilidad ISO/IEC 27001:2013.* El Anexo A es un documento que enlista los controles de seguridad establecidos en el estándar ISO/IEC 27001:2013 que contiene un conjunto de 114 controles agrupados en 35 objetivos de control.

El Anexo A es usualmente utilizado como un informe para la implementación de medidas de protección de la información, así como para evidenciar que no se están dejando de lado medidas de seguridad necesarias que no habían tenido encuenta dentro de una organización.

Entre los propósitos que desea alcanzar UNISANAR IPS a través de la implementación de controles es mejorar la seguridad de la información.

10.1.3 Niveles de madurez: Para UNISANAR IPS el nivel de madures tiene los siguientes 5 niveles:

10.1.4 Nivel 1, Control no Aplicable: Ese control no aplica a la entidad.

10.1.4.1 Nivel 2, Control no implementado: La organización aún no ha implementado medidas de seguridad.

10.1.4.2 Nivel 3, Control no cumple con el estándar: El control implementado no cumple con lo recomendado en la norma.

10.1.4.3 Nivel 4, Control Implementado sin documentar: Se encuentra con controles implementados, pero no documentado.

10.1.4.4 Nivel 5, Control Implementado y documentado: La organización cuenta con procedimientos documentados, aplica las mejoras de los procesos teniendo en cuenta los resultados de la auditoría de los procedimientos y los controles revisados.

10.2 ANÁLISIS DEL ANEXO A DE LA ISO27001:2013

Esta unidad pretende evidenciar los controles existentes y aquellos que son relevantes y aplicables para un adecuado SGSI en la organización y que aún no se han contemplado. En esta declaración, se encontrará las justificaciones pertinentes, motivo de selección, requisitos legales, obligaciones contractuales y necesidades empresariales de la organización en materia de seguridad de la información.

Tabla 21. Nomenclatura motivos de selección

NOMENCLATURA	NOMBRE
LR	Requerimiento Legales
CO	Obligación contractual
BR/BP	Requerimiento del negocio/Mejores prácticas adoptadas
RRA	Resultado de la evaluación de riesgos

Fuente: http://pegasus.javeriana.edu.co/~CIS0830IS12/documents/Anexo%20H%20Declaracion%20de%20Aplicabilidad.pdf

Tabla 22. Análisis de Políticas de Seguridad

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD	RAZONES PARA LA SELECCIÓN DE CONTROLES				JUSTIFICACIÓN
			LR	CO	BR/BP	RRA	
A.5 POLITICAS DE SEGURIDAD DE LA INFORMACIÓN							
A 5.1 ORIENTACIÓN DE LA DIRECCIÓN PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	A 5.1.1 POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	SI	X		X		La organización identifica los riesgos de información, se debe establecer una política para informar y concientizar a todas las partes sobre los riesgos a los que están expuestos. Se debe definir responsables, también debe ser revisada para asegurar la idoneidad con respecto a los riesgos.
	A 5.1.2 REVISIÓN DE LAS POLITICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	SI	X		X		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. 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.

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD	RAZONES PARA LA SELECCIÓN DE CONTROLES				JUSTIFICACIÓN
			LR	CO	BR/BP	RRA	
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN							
A 6.1 ORGANIZACIÓN INTERNA	A 6.1.1 ROLES Y RESPONSABILIDADES PARA LA SEGURIDAD DE LA INFORMACIÓN	SI			X		Se establece el compromiso, organización y asignación de responsabilidades para su cumplimiento, velar por mantener protegido su información mediante la revisión del sistema de gestión, firma de acuerdos de confidencialidad, tener contacto con las autoridades y la revisión independiente de seguridad de la información, se establecen controles para la organización interna de la seguridad de la información.
	A 6.1.2 SEPARACIÓN DE DEBERES	SI			X		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.
	A 6.1.3 CONTACTO CON LAS AUTORIDADES	SI	X				Se deberían mantener los contactos apropiados con las autoridades pertinentes. La Organización deberá establecer y mantener un contacto permanente con autoridades relevantes.
	A 6.1.4 CONTACTO CON GRUPOS DE INTERÉS ESPECIAL	SI			X		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

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD	RAZONES PARA LA SELECCIÓN DE CONTROLES				JUSTIFICACIÓN
			LR	CO	BR/BP	RRA	
							obtener información actualizada y, asesoría frente a un incidente de seguridad, que comprometa la Seguridad Informática.
	A 6.1.5 SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS.	SI				X	La Organización deberá aplicar todas y cada una de las políticas establecidas en la presente declaración de aplicabilidad, para todos 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.
A 6.2 DISPOSITIVOS MÓVILES Y TELETRABAJO	A 6.2.1 POLÍTICA PARA DISPOSITIVOS MÓVILES	NO				X	No aplica el control en la entidad
	A 6.2.2 TELETRABAJO	NO				X	No aplica el control en la entidad
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS							
	A 7.1.1 SELECCIÓN	SI		X			

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD	RAZONES PARA LA SELECCIÓN DE CONTROLES				JUSTIFICACIÓN
			LR	CO	BR/BP	RRA	
A 7.1 ANTES DE ASUMIR EL EMPLEO							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 las 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.
	A 7.1.2 TÉRMINOS Y CONDICIONES DEL EMPLEO	SI		X			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.
A 7.2 DURANTE LA EJECUCIÓN DEL EMPLEO	A 7.2.1 RESPONSABILIDADES DE LA DIRECCIÓN	SI			X		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.
	A 7.2.2 TOMA DE CONCIENCIA, EDUCACIÓN Y FORMACIÓN EN LA SEGURIDAD DE LA INFORMACIÓN	SI			X		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.

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD	RAZONES PARA LA SELECCIÓN DE CONTROLES				JUSTIFICACIÓN
			LR	CO	BR/BP	RRA	
	A.7.2.3 PROCESO DISCIPLINARIO	SI		X			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.
A 7.3 TERMINACIÓN Y CAMBIO DE EMPLEO	A7.3.1 TERMINACIÓN O CAMBIO DE RESPONSABILIDADES DE EMPLEO	SI		X			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. 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.
A.8 GESTION DE ACTIVOS							
A 8.1 RESPONSABILIDAD POR LOS ACTIVOS	A 8.1.1 INVENTARIO DE ACTIVOS	SI			X		Todos los activos deberían estar claramente identificados, confeccionando y manteniendo un inventario con los más importantes.

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD	RAZONES PARA LA SELECCIÓN DE CONTROLES				JUSTIFICACIÓN
			LR	CO	BR/BP	RRA	
	A 8.1.2 PROPIEDAD DE LOS ACTIVOS	SI			X		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.
	A 8.1.3 USO ACEPTABLE DE LOS ACTIVOS	SI			X		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.
	A 8.1.4 DEVOLUCIÓN DE LOS ACTIVOS	SI			X		El Departamento de Gestión Humana para realizar la respectiva liquidación al terminar el contrato laboral deberá exigir una paz y salvo firmado por las oficinas: • Gestión documental • Control interno • Contabilidad • jefe inmediato
A 8.2 CLASIFICACIÓN DE LA INFORMACIÓN	A 8.2.1 CLASIFICACIÓN DE LA INFORMACIÓN	SI			X		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

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD	RAZONES PARA LA SELECCIÓN DE CONTROLES				JUSTIFICACIÓN
			LR	CO	BR/BP	RRA	
							impacto negativo si por cualquier abuso en su manejo pudiera provocar al negocio en términos financieros, administrativos o legales.
	A 8.2.2 ETIQUETADO DE LA INFORMACIÓN	SI				X	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.
	A 8.2.3 MANEJO DE ACTIVOS	SI				X	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.
A 8.3 MANEJO DE MEDIOS	A 8.3.1. GESTIÓN DE MEDIOS REMOVIBLES	SI				X	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.
	A 8.3.2 DISPOSICIÓN DE LOS MEDIOS	SI				X	El Departamento de Sistemas definirá procedimientos para la eliminación segura de los medios de información respetando la normatividad vigente.

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD	RAZONES PARA LA SELECCIÓN DE CONTROLES				JUSTIFICACIÓN
			LR	CO	BR/BP	RRA	
	A 8.3.3 TRANSFERENCIA DE MEDIOS FÍSICOS	SI			X		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. • 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.
A.9 CONTROL DE ACCESO							
A 9.1 REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO	A 9.1.1 POLÍTICA DE CONTROL DE ACCESO	SI	X		X		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. • 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

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD	RAZONES PARA LA SELECCIÓN DE CONTROLES				JUSTIFICACIÓN
			LR	CO	BR/BP	RRA	
							puestos de trabajo. • Administrar los derechos de acceso en un ambiente distribuido y de red, que reconozcan todos los tipos de conexiones disponibles.
	A 9.1.2 ACCESO A REDES Y A SERVICIOS EN RED	SI				X	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.
A 9.2 GESTIÓN DE ACCESO DE USUARIOS	A 9.2.1 REGISTRO Y CANCELACIÓN DEL REGISTRO DE USUARIOS	SI				X	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. • Entregar a los usuarios por escrito sus derechos de acceso.

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD	RAZONES PARA LA SELECCIÓN DE CONTROLES				JUSTIFICACIÓN
			LR	CO	BR/BP	RRA	
	A 9.2.2 SUMINSITRO DE ACCESO DE USUARIOS	SI			X		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 del 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.
	A 9.2.3 GESTIÓN DE DERECHOS DE ACCESO PRIVILEGIADO	SI			X		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.
	A 9.2.4 GESTIÓN DE LA INF. DE AUTENTICACIÓN SECRETA DE USUARIOS	NO			X		La asignación de contraseñas se controlará a través de un proceso de administración formal. • Requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto. • Garantizar que los usuarios cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan al sistema. La contraseña provisional 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.

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD	RAZONES PARA LA SELECCIÓN DE CONTROLES				JUSTIFICACIÓN
			LR	CO	BR/BP	RRA	
							• Almacenar las contraseñas sólo en sistemas informáticos protegidos. • Configurar los sistemas de tal manera que las contraseñas tengan 10 caracteres de longitud.
	A 9.2.5 REVISIÓN DE LOS DERECHOS DE ACCESO DE USUARIOS	SI				X	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.
	A 9.2.6 RETIRO O AJUSTE DE LOS DERECHOS DE ACCESO.	SI				X	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.
A 9.3 RESPONSABILIDADES DE LOS USUARIOS	A 9.3.1 USO DE INFORMACIÓN DE AUTENTICACIÓN SECRETA	SI				X	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

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD	RAZONES PARA LA SELECCIÓN DE CONTROLES				JUSTIFICACIÓN
			LR	CO	BR/BP	RRA	
							establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.
A 9.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES	A 9.4.1 RESTRICCIÓN DE ACCESO A LA INFORMACIÓN	SI				X	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.
	A 9.4.2 PROCEDIMIENTO DE INGRESO SEGURO.	SI			X	X	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.
	A 9.4.3 SISTEMA DE GESTIÓN DE CONTRASEÑAS.	SI			X	X	Los sistemas de gestión de contraseñas deberían ser interactivos y asegurar contraseñas de calidad. Los usuarios podrán acceder al servicio de contraseña informática mediante la validación de la misma, la cual es exclusividad de su propietario.

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD	RAZONES PARA LA SELECCIÓN DE CONTROLES				JUSTIFICACIÓN
			LR	CO	BR/BP	RRA	
	A 9.4.4 USO DE PROGRAMAS UTILITARIOS PRIVILEGIADOS	SI		X			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. Es por esto la importancia del uso de una cuenta para los usuarios con privilegios restringidos y otra para el personal de soporte con privilegios de administrador; con eso, se evita que los usuarios estándar puedan instalar software.
	A 9.4.5 CONTROL DE ACCESO A CODIGOS FUENTE DE PROGRAMAS	SI		X		X	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: o 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). o Verificar que el Analista Responsable que autoriza la solicitud de un programa fuente sea el designado para la

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD	RAZONES PARA LA SELECCIÓN DE CONTROLES				JUSTIFICACIÓN
			LR	CO	BR/BP	RRA	
							aplicación, rechazando el pedido en caso contrario. Registrar cada solicitud aprobada.
A. 10 CRIPTOGRAFIA							
A 10.1 CONTROLES CRIPTOGRAFICOS	A 10.1.1 POLÍTICA SOBRE USO DE CONTROLES CRIPTOGRÁFICOS	NO				X	No es necesario desarrollar e implementar una política que regule el uso de controles criptográficos para la protección de la información.
	A 10.1.2 GESTIÓN DE LLAVES	NO				X	No 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.
A. 11 SEGURIDAD FISICA Y DEL ENTORNO							
A 11.1 ÁREAS SEGURAS	A 11.1.1 PERÍMETRO DE SEGURIDAD FÍSICA	SI				X	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.
	A 11.1.2 CONTROLES DE ACCESO FÍSICOS	SI				X	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.

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD	RAZONES PARA LA SELECCIÓN DE CONTROLES				JUSTIFICACIÓN
			LR	CO	BR/BP	RRA	
	A 11.1.3 SEGURIDAD DE OFICINAS, RECINTOS E INSTALACIONES	SI			X		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.
	A 11.1.4 PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y AMBIENTALES	SI			X		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.

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD	RAZONES PARA LA SELECCIÓN DE CONTROLES				JUSTIFICACIÓN
			LR	CO	BR/BP	RRA	
	A 11.1.5 TRABAJO EN ÁREAS SEGURAS	SI			X		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.
	A 11.1.6 ÁREAS DE DESPACHO Y CARGA	SI			X		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.

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD	RAZONES PARA LA SELECCIÓN DE CONTROLES				JUSTIFICACIÓN
			LR	CO	BR/BP	RRA	
A 11.2 EQUIPOS	A 11.2.1 UBICACIÓN Y PROTECCION DE LOS EQUIPOS	SI			X	X	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.
	A 11.2.2 SERVICIOS DE SUMINSITRO	SI			X		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.
	A 11.2.3 SEGURIDAD EN EL CABLEADO	SI			X	X	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 dividida del cableado estructurado con el fin de evitar interferencias.

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD	RAZONES PARA LA SELECCIÓN DE CONTROLES				JUSTIFICACIÓN
			LR	CO	BR/BP	RRA	
	A 11.2.4 MANTENIMIENTO DE EQUIPOS	SI			X	X	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.
	A 11.2.5 RETIRO DE ACTIVOS	SI			X	X	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.

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD	RAZONES PARA LA SELECCIÓN DE CONTROLES				JUSTIFICACIÓN
			LR	CO	BR/BP	RRA	
	A 11.2.6 SEGURIDAD DE EQUIPOS Y ACTIVOS FUERA DE LAS INSTALACIONES	SI	X	X	X	X	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.
	A 11.2.7 DISPOSICIÓN SEGURA O REUTILIZACIÓN DE EQUIPOS	SI				X	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.
	A 11.2.8 EQUIPOS DE USUARIO DESATENDIDO	NO			X	X	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.

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD	RAZONES PARA LA SELECCIÓN DE CONTROLES				JUSTIFICACIÓN
			LR	CO	BR/BP	RRA	
	A 11.2.9 POLÍTICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA	SI		X			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.
A.12 SEGURIDAD DE LAS OPERACIONES							
A 12.1 PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES	A 12.1.1 PROCEDIMIENTOS DE OPERACIÓN DOCUMENTADOS	SI		X	X		La Organización a través de su Gerencia y el Departamento de Sistemas, documentará y mantendrá actualizados los procedimientos operativos identificados en esta política, los cuales deben ser solicitados por el área que los requiera y autorizados por el Departamento de Sistemas.
	A 12.1.2 GESTIÓN DE CAMBIOS	SI	X		X	X	Todo cambio deberá ser evaluado previamente en aspectos técnicos y de seguridad.
	A 12.1.3 GESTIÓN DE CAPACIDAD	SI	X		X		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.
	A 12.1.4 SEPARACION DE LOS AMBIENTES DE DESARROLLO, PRUEBAS Y OPERACIÓN.	NO	X		X	X	El software que utiliza la empresa es desarrollado, actualizado e implementado por terceros.
		SI			X		

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD	RAZONES PARA LA SELECCIÓN DE CONTROLES				JUSTIFICACIÓN
			LR	CO	BR/BP	RRA	
A 12.2 PROTECCION CONTRA CODIGOS MALICIOSOS	A.12.2.1 CONTROLES CONTRA CÓDIGOS MALICIOSOS						El Departamento de Sistemas definirá e implementará controles de detección y prevención para la protección contra software malicioso.
A 12.3 COPIAS DE RESPALDO	A 12.3.1 RESPALDO DE LA INFORMACIÓN	SI	X	X	X	X	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.
A 12.4 REGISTRO Y SEGUIMIENTO	A12.4.1 REGISTRO DE EVENTOS	SI			X	X	Se deberían producir, mantener y revisar periódicamente los registros relacionados con eventos de actividad del usuario, excepciones, fallas y eventos de Seguridad Informática. Se generarán registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad.
	A12.4.2 PROTECCIÓN DE LA INFORMACIÓN DE REGISTRO	SI			X	X	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.

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD	RAZONES PARA LA SELECCIÓN DE CONTROLES				JUSTIFICACIÓN
			LR	CO	BR/BP	RRA	
	A12.4.3 REGISTROS DEL ADMINSITRADOR Y DEL OPERADOR	SI			X	X	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.
	A12.4.4 SINCRONIZACIÓN DE RELOJES	SI			X	X	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.
A 12.5 CONTROL DE SOFTWARE OPERACIONAL	A 12.5.1 INSTALACIÓN DE SOFTWARE EN SISTEMAS OPERATIVOS	SI			X	X	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.
A 12.6 GESTION DE LA VULNERABILIDAD TÉCNICA	A 12.6.1 GESTIÓN DE LAS VULNERABILIDADES TÉCNICAS	SI				X	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

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD	RAZONES PARA LA SELECCIÓN DE CONTROLES				JUSTIFICACIÓN
			LR	CO	BR/BP	RRA	
							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.
	A 12.6.2 RESTRICCIÓN SOBRE LA INSTALACION DE SOFWARE	SI				X	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.
A 12.7 CONTROLES DE AUDITORIAS DE SISTEMAS DE INFORMACIÓN	A 12.7.1 CONTROLES DE AUDITORIAS DE SISTEMAS DE INFORMACIÓN	SI				X	La realización de actividades de auditoría que involucren verificaciones de los sistemas en producción, implica 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.
A. 13 SEGURIDAD DE LAS COMUNICACIONES							
A 13.1 GESTIÓN DE LA SEGURIDAD DE LAS REDES	A 13.1.1 CONTROLES DE REDES	SI		X	X		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.

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD	RAZONES PARA LA SELECCIÓN DE CONTROLES				JUSTIFICACIÓN
			LR	CO	BR/BP	RRA	
	A 13.1.2 SEGURIDAD DE LOS SERVICIOS DE RED	SI			X	X	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.
	A 13.1.3 SEPARACIÓN EN LAS REDES	SI			X	X	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.

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD	RAZONES PARA LA SELECCIÓN DE CONTROLES				JUSTIFICACIÓN
			LR	CO	BR/BP	RRA	
A 13.2 TRANSFERENCIA DE INFORMACIÓN	A 13.2.1 POLÍTICAS Y PROCEDIMIENTOS DE TRASNFERENCIA DE INFORMACIÓN	SI			X		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.
	A 13.2.2 ACUERDOS SOBRE TRASNFERENCIA DE INFORMACIÓN	SI			X		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.

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD	RAZONES PARA LA SELECCIÓN DE CONTROLES				JUSTIFICACIÓN
			LR	CO	BR/BP	RRA	
							• Información sobre la propiedad de la y las condiciones de su uso.
	A 13.2.3 MENSAJERIA ELECTRÓNICA	SI				X	El Departamento de Sistemas definirá y documentará normas y procedimientos claros con respecto al uso de la mensajería electrónica.
	A 13.2.4 ACUERDOS DE CONFIDENCIALIDAD O DE NO DIVULGACIÓN	SI				X	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.
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS							
A 14.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN	A 14.1.1 ÁNALISIS Y ESPECIFICACIÓN DE REQUISITOS DE SI	SI		X	X		Esta política aplica para incorporar controles de seguridad a los sistemas adquiridos por terceros, al igual que para las mejoras o actualizaciones que se realicen a los sistemas ya existentes.

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD	RAZONES PARA LA SELECCIÓN DE CONTROLES				JUSTIFICACIÓN
			LR	CO	BR/BP	RRA	
	A 14.1.2 SEGURIDAD DE SERVICIOS DE LAS APLICACIONES EN REDES PÚBLICAS	SI			X		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.
	A 14.1.3 PROTECCIÓN DE TRANSACCIONES DE LOS SERVICIOS DE LAS APLICACIONES	SI			X		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. 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.

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD	RAZONES PARA LA SELECCIÓN DE CONTROLES				JUSTIFICACIÓN
			LR	CO	BR/BP	RRA	
A 14.2 CONTROL DE ACCESO AL SISTEMA OPERATIVO	A 14.2.1 POLÍTICA DE DESARROLLO SEGURO	NO			X	X	La Organización velará porque el desarrollo 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. Además, se asegurará que todo software adquirido externamente cuente con el nivel de soporte requerido por la Organización.
	A 14.2.2 PROCEDIMIENTO DE CONTROL DE CAMBIOS EN SISTEMAS	SI				X	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.

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD	RAZONES PARA LA SELECCIÓN DE CONTROLES				JUSTIFICACIÓN
			LR	CO	BR/BP	RRA	
	A 14.2.3 REVISIÓN TÉCNICAS DE LAS APLICACIONES DESPUES DE CAMBIOS EN LA PLATAFORMA DE OPERACIÓN	SI		X	X		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.
	A 14.2.4 RESTRICCIONES EN LOS CAMBIOS A LOS PAQUETES DE SOFTWARE	SI		X			Todos los cambios se deberían controlar estrictamente. 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

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD	RAZONES PARA LA SELECCIÓN DE CONTROLES				JUSTIFICACIÓN
			LR	CO	BR/BP	RRA	
							por si fuera necesario aplicarlo a nuevas versiones.
	A 14.2.5 PRINCIPIOS DE CONSTRUCCIÓN DE LOS SISTEMAS SEGUROS	SI		X			El Área de Sistemas de la Organización aplicará los principios de sistemas seguros, documentando y aplicando procesos seguros en la implementación de cualquier sistema de información.
	A 14.2.6 AMBIENTE DE DESARROLLO SEGURO	NO			X		Los desarrolladores que cuenta UNISANAR son externos.
	A 14.2.7 DESARROLLO CONTRATADO EXTERNAMENTE	SI		X			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 (Ver objetivo 18.1.2 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).

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD	RAZONES PARA LA SELECCIÓN DE CONTROLES			JUSTIFICACIÓN
			LR	CO	BR/BP	RRA
	A 14.2.8 PRUEBAS DE SEGURIDAD DE SISTEMAS	SI			X	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.
	A 14.2.9 PRUEBAS DE ACEPTACIÓN DE SISTEMAS	SI			X	El Departamento de Sistemas deberá establecer los requisitos para poner en producción un sistema nuevo o una actualización a un sistema ya existente.
A 14.3 DATOS DE PRUEBA	A14.3.1 PROTECCIÓN DE DATOS DE PRUEBA	SI			X	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.
A.15 RELACIONES CON LOS PROVEEDORES						
A. 15.1 RELACIONES CON LOS PROVEEDORES	A 15.1.1 SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES	SI		X		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).

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD	RAZONES PARA LA SELECCIÓN DE CONTROLES				JUSTIFICACIÓN
			LR	CO	BR/BP	RRA	
							• 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.
	A 15.1.2 TRATAMIENTO DE LA SEGURIDAD DENTRO DE LOS ACUERDOS CON PROVEEDORES	SI			X		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.
	A 15.1.3 CADENA DE SUMINISTRO DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN	SI			X		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.
A 15.2 GESTIÓN DE LA PRESENTACIÓN DE SERVICIOS DE PROVEEDORES	A 15.2.1 SEGUIMIENTO Y REVISIÓN DE LOS SERVICIOS DE LOS PROVEEDORES	SI			X		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

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD	RAZONES PARA LA SELECCIÓN DE CONTROLES				JUSTIFICACIÓN
			LR	CO	BR/BP	RRA	
							aceptado por el tercero, bajo las condiciones indicadas por la Organización.
	A 15.2.2 GESTIÓN DE CAMBIOS EN LOS SERVICIOS DE LOS PROVEEDORES	SI			X		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.
A.16 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION							
A 16.1 GESTION DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN	A 16.1.1 RESPONSABILIDADES Y PROCEDIMIENTOS	SI			X		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).
	A 16.1.2 REPORTE DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN	SI				X	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.
	A 16.1.3 REPORTE DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	SI				X	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

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD	RAZONES PARA LA SELECCIÓN DE CONTROLES				JUSTIFICACIÓN
			LR	CO	BR/BP	RRA	
							realizadas por el personal designado para tal fin.
	A 16.1.4 EVALUACIÓN DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN Y	SI			X		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.
	A 16.1.5 RESPUESTA A INCIDENTES DE SEGUIRIDAD DE LA INFORMACIÓN	SI			X		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.
	A 16.1.6 APRENDIZAJE OBTENIDO DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	SI			X		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.

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD	RAZONES PARA LA SELECCIÓN DE CONTROLES			JUSTIFICACIÓN
			LR	CO	BR/BP	RRA
	A 16.1.7 RECOLECCIÓN DE EVIDENCIA	NO			X	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.
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACION DE LA GESTION DE CONTINUIDAD DE NEGOCIO						
A 17.1 CONTINUIDAD EN SEGURIDAD DE LA INFORMACIÓN	A 17.1.1 PLANIFICACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	SI		X		La organización debería determinar los requisitos para la Seguridad Informática y su gestión durante situaciones adversas como situaciones de crisis o de desastre.
	A 17.1.2 IMPLEMENTACIÓN DE LA CONTINUIDAD DE LA SI	SI		X		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.
	A 17.1.3 VERIFICACIÓN, REVISIÓN Y EVALUACIÓN DE LA CONTINUIDAD DE LA SI	SI		X		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.

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD	RAZONES PARA LA SELECCIÓN DE CONTROLES				JUSTIFICACIÓN
			LR	CO	BR/BP	RRA	
A 17.2 REDUNDANIAS	A 17.2.1 DISPONIBILIDAD DE INSTALACIONES DE PROCESAMIENTO DE INFORMACIÓN	SI			X	X	La Organización propenderá por la existencia de una plataforma tecnológica redundante que satisfaga los requerimientos de disponibilidad aceptables para la misma.
A. 18 CUMPLIMIENTO							
A 18.1 CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES	A 18.1.1 IDENTIFICACIÓN DE LA LEGISLACIÓN APLICABLE Y DE LOS REQUISITOS CONTRACTUALES	SI			X		La Organización está obligada a cumplir la normatividad vigente que rige para el Sistema de Compensación Familiar del país, como lo es la Ley 21 de 1982, la Ley 789 de 2002 y el Decreto Reglamentario 341 de 1988, así como cualquier reglamentación que emane el gobierno nacional y que impacte directamente en el sistema. Dado que la Organización es una organización privada, todos sus documentos están sometidos a reserva, salvo excepciones de ley.
	A 18.1.2 DERECHOS DE PROPIEDAD INTELECTUAL	SI			X		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.
	A 18.1.3 PROTECCIÓN DE REGISTROS	SI		X			Toda información soportada por la infraestructura de tecnología informática de la Organización deberá ser almacenada y

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD	RAZONES PARA LA SELECCIÓN DE CONTROLES				JUSTIFICACIÓN
			LR	CO	BR/BP	RRA	
							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.
	A 18.1.4 PRIVACIDAD Y PROTECCIÓN DE INFORMACIÓN DE DATOS PERSONALES	SI			X		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.
	A 18.1.5 REGLAMENTACIÓN DE CONTROLES CRIPTOGRÁFICOS	NO				X	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

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD	RAZONES PARA LA SELECCIÓN DE CONTROLES				JUSTIFICACIÓN
			LR	CO	BR/BP	RRA	
							1999, el Decreto 1747 de 2000 y la Circular 10 de la Superintendencia de Industria y Comercio.
A 18.2 REVISIONES DE SEGURIDAD DE LA INFORMACIÓN	A 18.2.1 REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN	SI	X		X		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.
	A 18.2.2 CUMPLIMIENTO CON LAS POLÍTICAS Y NORMAS DE SEGURIDAD	SI	X		X		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.

OBJETIVOS DE CONTROL	CONTROLES ISO 27001: 2013	APLICABILIDAD	RAZONES PARA LA SELECCIÓN DE CONTROLES				JUSTIFICACIÓN
			LR	CO	BR/BP	RRA	
	A 18.2.3 REVISIÓN DEL SI CUMPLIMIENTO TÉCNICO		X		X		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. El resultado de la evaluación debe quedar consignado en un informe técnico para su interpretación por parte de los especialistas. 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. Las verificaciones de cumplimiento sólo serán realizadas por personas competentes, formalmente autorizadas y bajo la supervisión.

Fuente: El autor

10.3 LISTA DE CHEQUEO

Las listas de chequeo permiten realizar un primer inventario o verificación de las características de la empresa. Esta herramienta permite identificar puntos débiles, así como oportunidades de mejora a través de la verificación de un listado de aspectos presentes o no en el área a revisar. Pueden aplicarse en las diferentes actividades de la empresa.

Las listas de chequeo están compuestas por una serie de preguntas que permiten identificar los posibles problemas, causas y medidas apropiadas en los ámbitos temáticos que maneja cada lista. Incluyen preguntas claves y sub preguntas, las primeras ayudarán a encontrar las oportunidades para la implementación de la medida operativa y las sub preguntas ayudarán a conocer de manera detallada aquellas acciones que podrían desarrollarse en cada área objeto de mejora. Para su aplicación realizamos un recorrido por UNISANAR IPS siguiendo todas las etapas de seguridad de la información.

Tabla 23. Proceso Auditoria

PROCESO: DEPARTAMENTO SEGURIDAD INFORMATICA Y LAS TECNOLOGIAS DE INFORMACION					
RESPONSABLE DEL PROCESO: JEFE DEPARTAMENTO SEGURIDAD INFORMATICA Y RESPONSABLE SISTEMAS DE INFORMACION					FECHA:
OBJETIVO DE LA AUDITORIA: Identificar el cumplimiento de los controles y procedimientos identificados dentro del análisis y tratamiento de riesgos, basados en la norma ISO/IEC 27001:2013.					
AUDITOR LIDER:		LETTY YANETH MORENO PALOMEQUE, YACIRY ENITH PALACIOS PALACIOS			
Nº	**CONTROL**	**ASPECTOS**	**RESPUESTAS**		**OBSERVACIONES**
			CUMPLE	**NO CUMPLE**	
1	Políticas de Seguridad de la Información	¿Cuenta la empresa con política de seguridad de la información?		X	
	Orientación de la dirección para la seguridad de la información	¿Se da a conocer la política de seguridad de la Información a los empleados?		X	
	Objetivo: Brindar Orientación y soporte, por parte d la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes	¿Se revisa las políticas para la seguridad de la información?		X	

Tabla 23 (Continuación)

PROCESO: DEPARTAMENTO SEGURIDAD INFORMATICA Y LAS TECNOLOGIAS DE INFORMACION					
RESPONSABLE DEL PROCESO: JEFE DEPARTAMENTO SEGURIDAD INFORMATICA Y RESPONSABLE SISTEMAS DE INFORMACION					FECHA:
OBJETIVO DE LA AUDITORIA: Identificar el cumplimiento de los controles y procedimientos identificados dentro del análisis y tratamiento de riesgos, basados en la norma ISO/IEC 27001:2013.					
AUDITOR LIDER:		LETTY YANETH MORENO PALOMEQUE, YACIRY ENITH PALACIOS PALACIOS			
Nº	**CONTROL**	**ASPECTOS**	**RESPUESTAS**		**OBSERVACIONES**
			CUMPLE	**NO CUMPLE**	
	Organización y seguridad de la información	¿Se definen las responsabilidades de la seguridad de información?		X	
	Organización Interna	¿Hay separación de deberes dentro de la empresa?		X	
2	*Establecer el marco de referencia de gestión para iniciar y controlar con la implementación y la operación de la seguridad de la información dentro de la organización.*	¿Se mantiene contacto con las autoridades pertinentes?	X		
		¿Tiene contacto con grupos de interés especial?	X		
		¿Realiza gestión de proyectos para tratar la seguridad de la información?		X	

Tabla 23. (Continuación)

PROCESO: DEPARTAMENTO SEGURIDAD INFORMATICA Y LAS TECNOLOGIAS DE INFORMACION					
RESPONSABLE DEL PROCESO: JEFE DEPARTAMENTO SEGURIDAD INFORMATICA Y RESPONSABLE SISTEMAS DE INFORMACION					FECHA:
OBJETIVO DE LA AUDITORIA: Identificar el cumplimiento de los controles y procedimientos identificados dentro del análisis y tratamiento de riesgos, basados en la norma ISO/IEC 27001:2013.					
AUDITOR LIDER:		LETTY YANETH MORENO PALOMEQUE, YACIRY ENITH PALACIOS PALACIOS			
Nº	**CONTROL**	**ASPECTOS**	**RESPUESTAS**		**OBSERVACIONES**
			CUMPLE	**NO CUMPLE**	
3	Seguridad en los recursos humanos Durante la ejecución del empleo *Asegurarse que los empleados y contratistas tomen conciencia de sus responsabilidades en SI y las cumplan*	¿Existe responsabilidad de la dirección para exigir a los empleados a la aplicación de la SÍ? ¿Se realizan capacitaciones en toma de conciencia a los empleados, contratistas y la dirección? ¿Se realiza proceso disciplinario a los empleados que violen la Seguridad de la Información?	X	X X	

Tabla 23. (Continuación)

PROCESO: DEPARTAMENTO SEGURIDAD INFORMATICA Y LAS TECNOLOGIAS DE INFORMACION					
RESPONSABLE DEL PROCESO: JEFE DEPARTAMENTO SEGURIDAD INFORMATICA Y RESPONSABLE SISTEMAS DE INFORMACION				FECHA:	
OBJETIVO DE LA AUDITORIA: Identificar el cumplimiento de los controles y procedimientos identificados dentro del análisis y tratamiento de riesgos, basados en la norma ISO/IEC 27001:2013.					
AUDITOR LIDER:		LETTY YANETH MORENO PALOMEQUE, YACIRY ENITH PALACIOS PALACIOS			
Nº	**CONTROL**	**ASPECTOS**	**RESPUESTAS**		**OBSERVACIONES**
			CUMPLE	**NO CUMPLE**	
4	Gestión de activos	¿Existe un inventario donde se identifique los activos de la empresa?	X		
	- Responsabilidad por los activos	¿Se tiene destinado a quien pertenece cada activo?		X	
	- Clasificación de la Información.	¿Los empleados devuelven los activos una vez terminado el contrato con la empresa?		X	
	Manejo de Medios	¿Se clasifica la información teniendo en cuenta las responsabilidades?	X		
	- *Establecer el marco de referencia de gestión para iniciar y controlar con la implementación y la operación de la seguridad de la información dentro de la organización.*	¿Se etiqueta la información de acuerdo con el esquema de clasificación?		X	
	- *Asegurar que la información recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.*	¿Hay procedimientos para el manejo de activos?		X	
	- *Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios.*	¿Existen procedimientos para la gestión de medios removibles?		X	
		¿Hay procedimientos formales para disponer los medios cuando ya no se requieran?		X	
		¿Se protegen los medios físicos que contiene información?		X	

Tabla 23. (Continuación)

PROCESO: DEPARTAMENTO SEGURIDAD INFORMATICA Y LAS TECNOLOGIAS DE INFORMACION					
RESPONSABLE DEL PROCESO: JEFE DEPARTAMENTO SEGURIDAD INFORMATICA Y RESPONSABLE SISTEMAS DE INFORMACION					FECHA:
OBJETIVO DE LA AUDITORIA: Identificar el cumplimiento de los controles y procedimientos identificados dentro del análisis y tratamiento de riesgos, basados en la norma ISO/IEC 27001:2013.					
AUDITOR LIDER:		LETTY YANETH MORENO PALOMEQUE, YACIRY ENITH PALACIOS PALACIOS			
Nº	**CONTROL**	**ASPECTOS**	**RESPUESTAS**		**OBSERVACIONES**
			CUMPLE	**NO CUMPLE**	
5	Control de acceso	¿Existe una política de control de acceso con base en los requisitos del negocio y la seguridad de la información?		×	
	- Requisitos del Negocio para el control de acceso.	¿La empresa ha establecido roles para el acceso a redes y a servicios de red?		×	
	- Gestión de Acceso a Usuarios	¿Tienen proceso de registro y cancelación de usuarios?	×		
	- Responsabilidad de los usuarios	¿Se tiene procesos de suministro de acceso a usuarios?		×	
	Control de Acceso a Sistemas y Aplicaciones	¿Hay restricción de acceso a información?	×		
	- *Limitar el acceso a la información y a instalaciones de procesamiento de información.*	¿Cumplen con el uso de información autenticada secreta?		×	
	- *Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.*	¿Existen controles para el acceso al código fuente de programas?		×	
	- *Hacer que los usuarios rindan cuentas por la salvaguarda de la información de autenticación.*	¿Existe una política de control de accesos?		×	
	Evitar el acceso no autorizado a sistemas y aplicaciones.	¿Existe un procedimiento formal de registro y baja de accesos?		×	
		¿Se controla y restringe la asignación y uso de privilegios?		×	
		¿Existe una gestión de las contraseñas de		×	
		¿Existe una revisión de los derechos de acceso de los usuarios?		×	

Tabla 23. (Continuación)

PROCESO: DEPARTAMENTO SEGURIDAD INFORMATICA Y LAS TECNOLOGIAS DE INFORMACION					
RESPONSABLE DEL PROCESO: JEFE DEPARTAMENTO SEGURIDAD INFORMATICA Y RESPONSABLE SISTEMAS DE INFORMACION					FECHA:
OBJETIVO DE LA AUDITORIA: Identificar el cumplimiento de los controles y procedimientos identificados dentro del análisis y tratamiento de riesgos, basados en la norma ISO/IEC 27001:2013.					
AUDITOR LIDER:		LETTY YANETH MORENO PALOMEQUE, YACIRY ENITH PALACIOS PALACIOS			
Nº	**CONTROL**	**ASPECTOS**	**RESPUESTAS**		**OBSERVACIONES**
			CUMPLE	**NO CUMPLE**	
6	Criptografía Controles Criptográficos *Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.*	¿Existe una política de uso de controles		X	
		¿La empresa cuenta con política sobre uso de llaves criptográficas?		X	
		¿Existe métodos para tratar la protección de claves criptográficas y la recuperación de información?		X	

Tabla 23. (Continuación)

PROCESO: DEPARTAMENTO SEGURIDAD INFORMATICA Y LAS TECNOLOGIAS DE INFORMACION					
RESPONSABLE DEL PROCESO: JEFE DEPARTAMENTO SEGURIDAD INFORMATICA Y RESPONSABLE SISTEMAS DE INFORMACION					FECHA:
OBJETIVO DE LA AUDITORIA: Identificar el cumplimiento de los controles y procedimientos identificados dentro del análisis y tratamiento de riesgos, basados en la norma ISO/IEC 27001:2013.					
AUDITOR LIDER:		LETTY YANETH MORENO PALOMEQUE, YACIRY ENITH PALACIOS PALACIOS			
Nº	**CONTROL**	**ASPECTOS**	**RESPUESTAS**		**OBSERVACIONES**
			CUMPLE	**NO CUMPLE**	
7	Seguridad física y del entorno - Áreas Seguras. - Equipos. - *Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.* *Prevenir la perdida, daño, robo o compromiso de activos y la interrupción de las operaciones de la organización*	¿Cuenta la empresa con lugares de acceso restringido?		X	
		¿Hay control de Seguridad de acceso a lugares restringidos?		X	
		¿Se ha encontrado alguna falla en el control?		X	
		¿Tiene plan ante la falla del sistema de seguridad?		X	
		¿Se registran las personas que ingresan a las instalaciones de la empresa?		X	
		¿Se encuentra definido el perímetro de Seguridad Física?		X	
		¿Existe Política de control de Acceso a las Instalaciones?		X	
		¿Hay mecanismos de protección frente a amenazas externas?		X	
		¿Se trabaja en áreas seguras?		X	
		¿Existen control para el acceso a l área despacho y cargue?		X	
		¿Existe protección del cableado de energía eléctrica y de telecomunicaciones?		X	
		¿Hay política de equipos desatendidos?		X	
		¿Cuentan con política de escritorio limpio?		X	
		¿Se controla el retiro de activos en la empresa?		X	

Tabla 23. (Continuación)

PROCESO: DEPARTAMENTO SEGURIDAD INFORMATICA Y LAS TECNOLOGIAS DE INFORMACION					
RESPONSABLE DEL PROCESO: JEFE DEPARTAMENTO SEGURIDAD INFORMATICA Y RESPONSABLE SISTEMAS DE INFORMACION					FECHA:
OBJETIVO DE LA AUDITORIA: Identificar el cumplimiento de los controles y procedimientos identificados dentro del análisis y tratamiento de riesgos, basados en la norma ISO/IEC 27001:2013.					
AUDITOR LIDER:		LETTY YANETH MORENO PALOMEQUE, YACIRY ENITH PALACIOS PALACIOS			
Nº	**CONTROL**	**ASPECTOS**	**RESPUESTAS**		**OBSERVACIONES**
			CUMPLE	**NO CUMPLE**	
8	Seguridad de las operaciones - Procedimientos - Protección Contra Códigos maliciosos. - Registro y - Control de - Gestión de la Vulnerabilidad Técnica - *Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.* - *Asegurarse de que la información y las instalaciones de procesamiento de la información estén protegidas contra códigos maliciosos.* - *Registrar eventos y generar evidencia.* - *Asegurarse de la integridad de los sistemas operacionales.* *Prevenir el aprovechamiento de las vulnerabilidades técnicas.*	¿Tiene plan para protección de registros? ¿Se establece condiciones y términos de ¿Hace control para evitar la propagación de código Malicioso? ¿Utiliza medida de protección de los ¿Existe Manual de procedimientos ¿Existe manual de políticas de respaldo de la información? ¿Evalúa periódicamente los sistemas de información en busca de vulnerabilidades? ¿Existe manual de procedimientos y restricción para controlar la instalación de software? ¿Existen medidas de protección para contrarrestar las vulnerabilidades? ¿Existe plan de auditoria donde se implementa control, establecimiento de requisitos y actividades de auditoria?	X	X X X X X X X X X X	

Tabla 23. (Continuación)

PROCESO: DEPARTAMENTO SEGURIDAD INFORMATICA Y LAS TECNOLOGIAS DE INFORMACION					
RESPONSABLE DEL PROCESO: JEFE DEPARTAMENTO SEGURIDAD INFORMATICA Y RESPONSABLE SISTEMAS DE INFORMACION					FECHA:
OBJETIVO DE LA AUDITORIA: Identificar el cumplimiento de los controles y procedimientos identificados dentro del análisis y tratamiento de riesgos, basados en la norma ISO/IEC 27001:2013.					
AUDITOR LIDER:		LETTY YANETH MORENO PALOMEQUE, YACIRY ENITH PALACIOS PALACIOS			
Nº	**CONTROL**	**ASPECTOS**	**RESPUESTAS**		**OBSERVACIONES**
			CUMPLE	**NO CUMPLE**	
9	Seguridad de las comunicaciones	¿Existen controles sobre las redes y en la seguridad de los servicios de red?		X	
	- Gestión de la Seguridad de Redes	¿Se establecen las responsabilidades y los procedimientos para la gestión de equipos remotos, incluyendo los equipos en áreas de usuarios?		X	
	Transferencia de Información.	¿Establecer el registro y monitoreo adecuados para permitir el registro de acciones de seguridad pertinentes?		X	
	- Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.	¿Existen políticas, procedimientos y controles para la transferencia de la información?		X	
	Mantener la Seguridad de la información Transferida dentro de una organización.	¿Existen acuerdos de confidencialidad o de no divulgación para la transferencia de la información?		X	
		¿Existen controles que garanticen la seguridad incluida en la mensajería electrónica?		X	

Tabla 23. (Continuación)

PROCESO: DEPARTAMENTO SEGURIDAD INFORMATICA Y LAS TECNOLOGIAS DE INFORMACION					
RESPONSABLE DEL PROCESO: JEFE DEPARTAMENTO SEGURIDAD INFORMATICA Y RESPONSABLE SISTEMAS DE INFORMACION					FECHA:
OBJETIVO DE LA AUDITORIA: Identificar el cumplimiento de los controles y procedimientos identificados dentro del análisis y tratamiento de riesgos, basados en la norma ISO/IEC 27001:2013.					
AUDITOR LIDER:		LETTY YANETH MORENO PALOMEQUE, YACIRY ENITH PALACIOS PALACIOS			
Nº	**CONTROL**	**ASPECTOS**	**RESPUESTAS**		**OBSERVACIONES**
			CUMPLE	**NO CUMPLE**	
	Adquisición, desarrollo y mantenimiento de los sistemas de información	¿Existen controles de seguridad en las redes públicas?		X	
	- Requisitos de seguridad de los sistemas de información.	¿Existen políticas para realizar análisis y especificaciones de requisitos de seguridad de la información?		X	
	- Seguridad en los procesos de desarrollo y de soporte.	¿Existe ambiente de desarrollo seguro?		X	
	Datos de Prueba	¿Existen controles de restricción sobre cambios a paquetes de software?		X	
10	- *Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo.*	¿Existe política para desarrollo de software seguro?		X	
	Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información	¿Hay política para realización de pruebas que incluye aceptación y de seguridad de sistemas?		X	

Tabla 23. (Continuación)

PROCESO: DEPARTAMENTO SEGURIDAD INFORMATICA Y LAS TECNOLOGIAS DE INFORMACION					
RESPONSABLE DEL PROCESO: JEFE DEPARTAMENTO SEGURIDAD INFORMATICA Y RESPONSABLE SISTEMAS DE INFORMACION					FECHA:
OBJETIVO DE LA AUDITORIA: Identificar el cumplimiento de los controles y procedimientos identificados dentro del análisis y tratamiento de riesgos, basados en la norma ISO/IEC 27001:2013.					
AUDITOR LIDER:		LETTY YANETH MORENO PALOMEQUE, YACIRY ENITH PALACIOS PALACIOS			
Nº	**CONTROL**	**ASPECTOS**	**RESPUESTAS**		**OBSERVACIONES**
			CUMPLE	**NO CUMPLE**	
11	Relación con los proveedores - Seguridad de información en las relaciones con los proveedores. Gestión de la prestación de servicios de proveedores. - *Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.* *Mantener nivel acordado de seguridad de la información y de prestación de servicios en línea con los acuerdos con los proveedores.*	¿Existe una política de seguridad de la información para proveedores?		X	
		¿Procedimientos para hacer seguimiento y revisión de los servicios de los proveedores?		X	
		¿Están claramente definidos los requisitos legales y de reglamentación, incluida la protección de datos, los derechos de propiedad intelectual y derechos de autor, y una descripción de cómo se asegurará que se cumplan?	X		
		¿Existen acuerdos con proveedores que incluyen requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación?	X		

Tabla 23. (Continuación)

PROCESO: DEPARTAMENTO SEGURIDAD INFORMATICA Y LAS TECNOLOGIAS DE INFORMACION					
RESPONSABLE DEL PROCESO: JEFE DEPARTAMENTO SEGURIDAD INFORMATICA Y RESPONSABLE SISTEMAS DE INFORMACION					FECHA:
OBJETIVO DE LA AUDITORIA: Identificar el cumplimiento de los controles y procedimientos identificados dentro del análisis y tratamiento de riesgos, basados en la norma ISO/IEC 27001:2013.					
AUDITOR LIDER:		LETTY YANETH MORENO PALOMEQUE, YACIRY ENITH PALACIOS PALACIOS			
Nº	**CONTROL**	**ASPECTOS**	**RESPUESTAS**		**OBSERVACIONES**
			CUMPLE	**NO CUMPLE**	
	Gestión de incidentes de seguridad de la información	¿Establecen responsabilidades y procedimientos de gestión dar respuesta a los incidentes y debilidad de la seguridad de la información?		X	
	Gestión de incidentes y mejoras en la seguridad de la información	¿Existen canales apropiados para dar reportes de eventos de seguridad de información?		X	
12	*Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información incluida la comunicación sobre eventos de seguridad y debilidades.*	¿Realizan evaluación de eventos de seguridad de la información?		X	
		¿Existen procedimientos para recolección, identificación que puedan servir como evidencia?		X	

Tabla 23. (Continuación)

PROCESO: DEPARTAMENTO SEGURIDAD INFORMATICA Y LAS TECNOLOGIAS DE INFORMACION					
RESPONSABLE DEL PROCESO: JEFE DEPARTAMENTO SEGURIDAD INFORMATICA Y RESPONSABLE SISTEMAS DE INFORMACION					FECHA:
OBJETIVO DE LA AUDITORIA: Identificar el cumplimiento de los controles y procedimientos identificados dentro del análisis y tratamiento de riesgos, basados en la norma ISO/IEC 27001:2013.					
AUDITOR LIDER:		LETTY YANETH MORENO PALOMEQUE, YACIRY ENITH PALACIOS PALACIOS			
Nº	**CONTROL**	**ASPECTOS**	**RESPUESTAS**		**OBSERVACIONES**
			CUMPLE	**NO CUMPLE**	
13	Aspecto de seguridad de la información de la gestión de continuidad de negocio	¿Existe plan de continuidad del negocio en la empresa?		X	
	- Continuidad de seguridad de la información.	¿Existen procedimientos para la implementación de la continuidad de la seguridad de la información?		X	
	Redundancias.	¿Verifica los controles de continuidad de seguridad de la información?		X	
	- *La continuidad de la seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.*	¿Existe un mecanismo de planificación para la continuidad del negocio?		X	
	Asegurar la disponibilidad de instalaciones de procesamiento de información.			X	

Tabla 23. (Continuación)

PROCESO: DEPARTAMENTO SEGURIDAD INFORMATICA Y LAS TECNOLOGIAS DE INFORMACION					
RESPONSABLE DEL PROCESO: JEFE DEPARTAMENTO SEGURIDAD INFORMATICA Y RESPONSABLE SISTEMAS DE INFORMACION					FECHA:
OBJETIVO DE LA AUDITORIA: Identificar el cumplimiento de los controles y procedimientos identificados dentro del análisis y tratamiento de riesgos, basados en la norma ISO/IEC 27001:2013.					
AUDITOR LIDER:		LETTY YANETH MORENO PALOMEQUE, YACIRY ENITH PALACIOS PALACIOS			
Nº	**CONTROL**	**ASPECTOS**	**RESPUESTAS**		**OBSERVACIONES**
			CUMPLE	**NO CUMPLE**	
14	Cumplimiento - Cumplimiento de requisitos legales y contractuales. Revisiones de Seguridad de Información - *Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de información y de cualquier requisito de seguridad.* *Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales*	¿Se tiene identificada la legislación aplicable y de los requisitos contractuales?	X		
		¿Están definidos los procedimientos para establecer requisitos legales y de reglamentación, incluida la protección de datos, los derechos de propiedad intelectual y derechos de autor?		X	
		¿Existe política de para asegurar la privacidad y la protección de la información como lo exige la legislación?		X	
		¿Se usan los controles criptográficos?		X	
		¿Se revisa periódicamente la seguridad de la información?		X	
		¿Cumple con las políticas y normas de		X	
		¿Se revisa periódicamente los sistemas de información para determinar el cumplimiento con las políticas y normas de seguridad de información?		X	
FIRMA RESPONSABLE DEL PROCESO			FIRMA AUDITOR LIDER		

Fuente: El autor

La situación actual en la IPS UNISANAR en cuanto al tema de seguridad informática es la siguiente:

No existe instrucción o cultura sobre la protección y el uso de la información sobre los riesgos a los que puede llegar ser expuestos por su mal uso.

Aunque se tiene una clasificación de acuerdo con las funciones que se cumplen, no se tiene constantemente a la mano en algunas dependencias para un fácil acceso y control de la misma.
En lo revisado no se conoce un inventario de los activos de la empresa actualizado, ni los responsables de su uso.
Utilizan equipos personales dentro de la instalación con información confidencial de la empresa
No hay un monitoreo de acceso a los equipos e información.
No se tiene capacitado al personal para un eventual riesgo en cuanto a prevención o cómo reaccionar ante dichas amenazas.
No se observa compromiso para garantizar la confidencialidad, integridad y disponibilidad de la información en algunas dependencias.
No emplean correos institucionales para enviar o recibir la informacion.

Análisis-Seguridad de instalaciones físicas

El edificio no cuenta con cámara de vigilancia, ni con control de acceso al edificio, no existe un control de acceso en los horarios no hábiles de la empresa, ni un control adecuado sobre sus visitantes.

10.4 ANALISIS DE LA INFORMACIÓN

En esta fase se va a analizar la información, teniendo en cuenta los datos obtenidos en la fase anterior, identificando las amenazas, riesgos y vulnerabilidad a la que están expuesta la información de UNISANAR IPS.

10.4.1 Identificación del Riesgo: Caracterización de las amenazas

Después de realizar el inventario de los activos con los que cuenta UNISANAR IPS vamos a establecer las amenazas a los que están expuestos los activos.

Las amenazas son hechos que ocurres y deben ser identificados a tiempos antes de que causen daño en los activos.

Las amenazas a las que se encuentra ostentada UNISANAR IPS se refleja en el siguiente cuadro:

Tabla 24. Identificación de las amenazas UNISANAR IPS

Ítem	Vulnerabilidades de seguridad	Amenazas de seguridad	Descripción de la amenaza
1	Fallas en el fluido eléctrico, permitiendo el apagado de los equipos sin previo aviso e inesperadamente. Falta de UPS	Daños en el hardware de los equipos Activos y de comunicación.	Generación de pérdida de información junto con el hardware.
2	Falta de actualización del Software (Sistema Operativo).	Permeabilidad del Sistema Operativo, Aplicaciones y Herramientas con respecto a los rotos (Agujeros) o ventanas traseras.	Acceso de los Hacker o Cracker malintencionados a la información confidencial y protegida. Falta de soporte en el Software.
3	Desconocimiento de los criterios de la seguridad informática de los Administrativos y funcionarios.	Administrativos y funcionarios débiles y de fácil penetración por ingeniería social.	Alcance de la información por ingeniería social. Falta de estrategias de prevención y predicción de ataques.
4	Uso de dispositivos de almacenamientos externos para el transporte de información (Pen Drive, etc.)	Rotación y propagación de virus con información y datos viciados.	Transporte de archivos, datos, y elementos informáticos dañinos para el sistema.
5	Instalación de software no licenciado y autorizado.	Instalación de Software, Herramientas y programas que Debilitan la seguridad del sistema.	Software y Herramientas con ventanas traseras, que rompen los protocolos de seguridad. A la vez expuesta a sanciones económicas por utilización de software no licenciado.

Tabla 24. (Continuación)

Ítem	Vulnerabilidades de seguridad	Amenazas de seguridad	Descripción de la amenaza
6	Falta de cableado estructurado (Equipos y Cables a la intemperie)	Perdida de información y bajo control de la misma. Equipos de comunicación y cableado vulnerables.	La mala distribución de equipos y cable permite vulnerabilidades y accesos no autorizados.
7	Falta de backup de Datos, Archivos e Información	Inexistencia en el almacenamiento de la información de respaldo.	La pérdida de información genera riesgos de seguridad.
8	Error en la configuración de las políticas de seguridad del Sistema.	Fragilidad y facilidad en la penetración en los sistemas de seguridad.	Los privilegios de las políticas de seguridad no se cumplen según los estructurados y permiten accesos inesperados.
9	Falla en el hardware de los equipos (Mantenimiento de Equipos)	El daño parcial o Total de los equipos permite la perdida de información,	La falta de mantenimiento preventivo y predictivo genera la reducción de la vida útil de los equipos.
10	Personal Administrativo o funcionarios en cuanto a la ingeniería social de hacker y/o Cracker.	Los funcionarios y Administrativos son vulnerables a razón de la información pertinente de la seguridad en la ingeniería social.	La filtración o falta de aplicación de políticas de seguridad que impidan el acceso a claves o contraseñas de los usuarios por falta de capacitación en prevención.

Tabla 24. (Continuación)

Ítem	Vulnerabilidades de seguridad	Amenazas de seguridad	Descripción de la amenaza
11	Control de Acceso al cuarto de comunicaciones de personal no autorizado.	El acceso a equipos y componentes de la red por personal no autorizado.	El acceso o manejo de equipos de la red sin el conocimiento indicado permiten la generación y debilidad en las redes.
12	Aplicación de políticas de seguridad a las contraseñas o Password de los Administrativos y funcionarios.	Las contraseñas y actualización periódica de las mismas no cumplen con las políticas de seguridad.	Fácil acceso e identificación de las contraseñas o Password.
13	Capacitación y actualización de los Administrativos y funcionarios en políticas de Seguridad Informática en el activo más importante de la empresa.	La falta de actualizaciones y capacitaciones de los funcionarios establecen criterios de inseguridad informática.	El desconocimiento de la seguridad informática y sus políticas generan vulnerabilidades en el sistema generados por los funcionarios.
14	Conectividad WI-FI de cualquier equipo externo a la red corporativa.	La falta de configuración para limitar el acceso a la red inalámbrica	Cualquier miembro externo o interno puede acceder a la infraestructura computacional de la empresa. Robo de información.

Fuente: Autor

En el siguiente cuadro se observa la identificación de los riesgos informáticos, categoría, vulnerabilidades, amenazas, recursos afectados, causas, controles internos, tratamiento de los riesgos y las acciones para la empresa UNISANAR IPS, con el fin de lograr implantar un adecuado manejo en la valoración de los activos informáticos.

Tabla 25. Identificación

RIESGOS	CATEGORIA	VULNERABILIDAD	AMENAZAS	RECURSOS AFECTADOS	CAUSAS	CONTROLES INTERNOS	TRATAMIENTO DE LOS RIESGOS	ACCIONES
Manipulación de terceros a información confidencial y privilegiada	Software	Fallas en los Sistemas Operativo	Perdida de programas e información valiosa, que afectan al software de facturación y contable INFOSALUD	Imagen Institucional	Mal manejo de los permisos de acceso	Privacidad y protección de Información Personal Identificable.	Realizar capacitaciones para la reducción de riesgos en cuanto a las políticas de seguridad	Capacitaciones a funcionarios de las políticas
Hurto de información	Personal	Suplantación de usuarios.	Utilización de información privilegiada para fines inadecuado	Imagen Institucional	Desconocimiento de políticas de seguridad	Seguridad de Recursos Humanos	Practica de seguridad de la información	Capacitar al personal que efectúe el tratamiento de datos personales.
Acceso no autorizado a información	Hardware	Fallas del hardware y sus componentes, , almacenamiento inadecuada, capacidad inadecuada, código malicioso.	Infección de sistemas de almacenamiento y manipulación de elementos periférico, falta de mantenimiento y extravío de equipos	Sistemas de información	Privilegio no adecuado en acceso	Política de control de accesos y elementos perifericos.	Practica de seguridad de la información	Capacitar al personal que efectúe el tratamiento de datos personales.

Tabla 25. (Continuación)

RIESGOS	CATEGORIA	VULNERABILIDAD	AMENAZAS	RECURSOS AFECTADOS	CAUSAS	CONTROLES INTERNOS	TRATAMIENTO DE LOS RIESGOS	ACCIONES
Errores de Usuarios	Servidor de Correo	Contraseñas fáciles	El poco cambio de contraseñas y la utilización de algunas sin seguridad que se conviertan en fáciles de adivinar	Sistemas de información	Usurpación de Usuario para el acceso a información	Política de uso de los controles criptográficos.	Protección mediante medios criptográficos e impedir el acceso a usuarios no autorizados	Técnicas y recomendaciones para el manejo de contraseñas
Mantenimiento de Software	Equipos Activos	Configuración de Servidores	Penetración a los sistemas desde cualquier ventana abierta	Desastre por la alteración de la información	Manipulación de contenidos confidenciales por terceros	Adquisición, desarrollo y mantenimiento de Sistemas.	Actualizar las medidas de seguridad y garantizar los sistemas de información	Mantenimiento continuo y actualizaciones de software autorizados
Desconocimiento de las políticas de Seguridad	Control de Información	Políticas de seguridad	Difusión de la información confidencial o hurto de la misma con fines diferentes a los establecidos	Sistemas de información	Manipulación de contenidos confidenciales por terceros	Políticas de Seguridad de la Información.	Practica de seguridad de la información	Capacitar al personal que efectúe el tratamiento de datos personales.

Tabla 25. (Continuación)

RIESGOS	CATEGORIA	VULNERABILIDAD	AMENAZAS	RECURSOS AFECTADOS	CAUSAS	CONTROLES INTERNOS	TRATAMIENTO DE LOS RIESGOS	ACCIONES
Destrucción de la información	Seguridad Lógica	Backup	Perdida de la información por falta de respaldo	Imagen institucional y toma de decisiones	Perdida de la Información	Copias de seguridad de la información.	Actividades para la ejecución de respaldos de información para prevenir la pérdida de información.	Respaldo de información
Adecuación y mantenimiento	Hardware	Instalación de UPS	Perdida de la información sin respaldo y daño a los equipos.	Retraso en los procesos	Falta de plan de mantenimiento	Perímetro de seguridad física.	Realizar un registro de los medios de almacenamiento de los datos personales	planes de recuperación de información inmediata y cubrimiento de equipos
Virus	Servicios	Privilegio de Instalación de Programas a todos los usuarios	Exponen el ingreso de software dañinos	Daño de la información y conectividad	Ataque a los sistemas por falta de actualización de antivirus	Controles contra el código malicioso.	Constante actualización de antivirus	Instalación de antivirus

Fuente: El autor

10.4.2 Evaluación de los riesgos: Las empresas hoy en día con todos sus avances tecnológicos, se ven obligadas a proteger la información de tal forma que se pueda conservar los principios de Confiabilidad, integridad, disponibilidad, es por esto que cada vez se les hace más compleja la protección de la misma por la cantidad de información que se va almacenando en el trascurso del tiempo.

Para la implementación de un Sistema Integrado de Gestión de Seguridad de la información, se hace necesario el inventario y clasificación de los activos a trabajar en la empresa, haciendo un análisis minucioso en todas las áreas que se requiera y así detectar los activos específicos a desarrollar, sus vulnerabilidades, amenazas, riesgos, impactos y como protegerla, todo esto se puede realizar mediante la implementación de MAGERIT.

Los análisis de riesgos son las utilizaciones de la información disponible con la que se pretende identificar cada uno de los peligros a los que se está expuesta la información, existen algunos conceptos de riesgos y análisis de riesgos y de la seguridad de la información tales como:

Amenazas: Causa potencial de un daño a un activo.
Vulnerabilidad: Debilidad de un activo que puede ser aprovechado por una amenaza
Impacto: Consecuencia de que la amenaza ocurra.
Riesgos intrínsecos: Calculo del daño probable a un activo si se encontrara desprotegido.
Salvaguardar: Medida técnica u organizativa que ayuda a paliar el riesgo.
Riesgos residuales: riesgos remanentes tras la aplicación de salvaguardas.[19]

[19] Poveda, José M. ISO 27001. [En línea] Marzo de 2011. https://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-8.pdf.

Con el fin de desarrollar un SGSI, y efectuar el análisis de riesgos de la UNISANAR IPS, mediante la metodología MAGERIT, se requiere adelantar algunos pasos fundamentales:

ACTIVOS

Siempre es necesario para realizar un análisis de riesgos, conocer sus activos, partiendo de un grupo que sea relevante y manejable, cada uno de esos activos deberán tener sus amenazas, las vulnerabilidades y el impacto con el que podres analizar cada uno de los riesgos.

10.4.3 Estimación del Riesgo

Tabla 26. Escala cualitativa y cuantitativa

ESCALA		
IMPACTO	PROBABILIDAD	RIESGO
MA: Muy Alto (4)	A: Probable (3)	MA: Critico
A: Alto (3)	M: Posible (2)	A: Importante
M: Medio (2)	B: Poco Probable (1)	M: Apreciable
B: Bajo (1)		B: Bajo

Fuente: El autor

Tabla 27. Nivel del Riesgo

Rango Inferior	**Nivel del Riesgo**	**Rango Superior**
0>=	B: Bajo	<=3
3>=	M: Apreciable	<=6
6>=	A: Importante	<=9
9>=	MA: Critico	<=12

Fuente: El autor

Tabla 28. Calcular el Nivel del Riesgo: IMPACTO X PROBABILIDAD

RIESGOS		**PROBABILIDAD**		
		A: Probable (3)	M: Posible (2)	B: Poco Probable (1)
IMPACTO	MA: Muy Alto (4)	MA=12	A=8	M=4
	A: Alto (3)	A=9	M=6	B=3
	M: Medio (2)	M=6	M=4	B=2
	B: Bajo (1)	B=3	B=2	B=1

Fuente: El autor

Tabla 29. Inventario de Activos

Tipo de activo	Activo	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Riesgos
Servicios	Servidores Web	Ataques de intrusos internos y externos	Acceso remoto	MA=4	M=1	M: Apreciable =4
	Servidores de Aplicación	Información confidencial accesible	Falta de mecanismos de monitoreo de la información	MA=4	A=3	MA: Critico =12
	Servidores DNS	Obtención de los nombres de dominio	configuración de seguridad predeterminada	A=3	M=2	M: Apreciable =6
	Servidores de Acceso Remoto Telefónico	Caída del servicio	Respuestas tardías a los clientes	A=3	M=3	A: Importante =9
	Servidores de Correo electrónico	El poco cambio de contraseñas y la utilización de algunas sin seguridad que se conviertan en fáciles de adivinar, el acceso a códigos maliciosos	Contraseñas fáciles	M=2	B=1	B: Bajo =2
	Servidores Proxy	Ataques de virus informáticos	Privilegio de Instalación de Programas a todos los usuarios	A=3	B=1	B: Bajo=3
	Impresoras	Hurto	Lentitud en la entrega de información	M=2	M=2	M: Apreciable =4

Tabla 29. (Continuación)

Tipo de activo	Activo	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Riesgos
Datos/ Información	Puntos de Accesos	Manipulación de la información y configuración	Acceso no Autorizado	M=2	M=2	M: Apreciable =4
	Bases de Datos	Manipulación de información de reserva	Acceso no Autorizado	MA=4	M=2	A: Importante =8
Aplicaciones (Software)	Sistemas Operativo Linux	Perdida de programas e información valiosa, que afectan al software	Mal manejo de Software, Alteración de información	A=3	M=2	M: Apreciable =6
	Sistema Operativo Windows	Mal manejo de Software, Alteración de información	Perdida de programas e información valiosa, que afectan al software	A=3	M=2	M: Apreciable =6
	Adobe	Alteración de información	Perdida de programas	M=2	M=2	M: Apreciable =4
Equipos informáticos	Computadores	Falla en los Equipos	Perdida de la información	A=3	A=3	A: Importante =9
(Hardware)	Video Beam	Hurto	Exponen el ingreso de software dañinos	M=2	A=3	M: Apreciable =6
	Equipos/ impresoras	Hurto	Exponen el ingreso de software dañinos	M=2	M=2	M: Apreciable =4

Tabla 29. (Continuación)

Tipo de activo	Activo	Amenazas	Vulnerabilidades	Impacto	Probabilidad	Riesgos
Redes de Comunicaciones	Router	Errores en su configuración	Corte de energía	M=2	M=2	M: Apreciable =4
	Firewall	Temperatura, borrado de información,	Corte de energía	M=2	M=2	M: Apreciable =4
Soportes de Información	Disco Duro	Falta de respaldo, borrado de información	Perdida de la información sin respaldo	A=3	A=3	A: Importante =9
	Memoria USB	Daños, borrado de información	Perdida de la información sin respaldo	A=3	A=3	A: Importante =9
Equipamiento Auxiliar	Sistema de alimentación Ininterrumpida	Fallas de UPS	Perdida de la información sin respaldo y daño a los equipos.	M=2	M=2	M: Medio =4
Instalaciones	Cableado Estructurado	Falla en el cableado	Usuarios sin servicio	A=3	A=3	A: Importante =9
Personal	Funcionarios de la Empresa	Conflictos internos, Falta de capacitación	Utilización de información privilegiada para fines inadecuado	MA=4	A=3	MA: Critico =12

Fuente: El autor

10.4.4 Plan de tratamiento del riesgo: Para dar soluciones y recomendaciones en el plan de tratamiento del riesgo, se seleccionaron los tipos de activos, los activos afectados, el nivel del riesgo con su grado de prioridad, y se procedió a salvaguardar mediante algunos mecanismos prácticos de desarrollar con las respectivas recomendaciones y las medidas a las que hay que llegar con el fin de minimizar los riesgos. De lo que se obtuvo el siguiente cuadro.

Tabla 30. Plan de Tratamiento de los Riesgos

Tipo de activo	Activo	Riesgos	Salvaguardas	Recomendación	Medidas
Servicios	Servidores Web	M: Apreciable =4	Políticas de control de acceso	Limitar el acceso a información y a instalaciones de procesamiento de información, establecimiento de privilegios y roles de usuario para el acceso	Evitar, Transferir y reducir los riesgos
	Servidores de Aplicación	MA: Critico =12	Restricción de acceso a la información	Controlar los derechos de acceso de los usuarios y otras aplicaciones	Evitar, Transferir los riesgos
	Servidores DNS	M: Apreciable =6	Protección de la información de registros	Se debe proteger la información de registro contra alteración y acceso no autorizado	Evitar, Asumir, Dispersar y atomizar, el Riesgo
	Servidores de Acceso Remoto Telefónico	A: Importante =9	Condiciones y términos del servicio	Constante mantenimiento de los equipos	Evitar, Transferir y reducir los riesgos
	Servidores de Correo electrónico	B: Bajo =2	Políticas de acceso y control de código malicioso	Segregación de los roles de control de acceso, asegurar la calidad y las contraseñas y el cambio, control de códigos maliciosos.	Evitar, Transferir y reducir los riesgos
	Servidores Proxy	B: Bajo=3	Políticas de control de acceso	Segregación de los roles de control de acceso, asegurar la calidad y las contraseñas y el cambio.	Evitar, Asumir, Dispersar y atomizar, reducir el Riesgo

Tabla 30. (Continuación)

Tipo de activo	Activo	Riesgos	Salvaguardas	Recomendación	Medidas
Datos/ Información	Puntos de Accesos	M: Apreciable =4	Control de redes	Establecer las responsabilidades y procedimientos para la gestión de equipos de redes, autenticar los sistemas de redes	Asumir, Dispersar y atomizar, reducir el Riesgo
	Bases de Datos	A: Importante =8	Copia de respaldos	Efectuar copias de respaldos periódicas, las cuales serán guardas en lugares remotos para su utilización posterior.	Dispersar y atomizar el riesgo
Aplicaciones (Software)	Sistema de Gestión de Proyectos	M: Apreciable =6	Protección contra códigos maliciosos, control de software	Prohibición de software no autorizados, se debería usar sistemas de control de la configuración de software y conservar la versión anterior como medidas de contingencias	Evitar, Transferir y reducir los riesgos
	Sistema Operativo Windows	M: Apreciable =6	Protección contra códigos maliciosos, control de software, instalación de firewall	Prohibición de software no autorizados, se debería usar sistemas de control de la configuración de software y conservar la versión anterior como medidas de contingencias	Evitar, Transferir y reducir los riesgos

Tabla 30. (Continuación)

Tipo de activo	Activo	Riesgos	Salvaguardas	Recomendación	Medidas
Equipos informáticos (Hardware)	Computadores	A: Importante =9	Servicio de suministro	Los equipos se deberán proteger contra fallas de energías, alarmas de mal funcionamiento de los equipos	Evitar, Transferir y Asumir el Riesgo
	Video Beam	M: Apreciable =6	Mantenimiento de equipos	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas	Evitar, Transferir y Asumir el Riesgo
	Equipos/ impresoras	M: Apreciable =4	Mantenimiento de equipos	Llevar registros de las fallas y mantenimientos preventivos y correctivos	Evitar, Transferir y Asumir el Riesgo
	Puestos de trabajo	B: Bajo =1	Mantenimiento de equipos y actualizaciones	Estricto control sobre los equipos informáticos que entran y salen de las instalaciones.	Evitar, Transferir y Asumir el Riesgo
Redes de comunicaciones	Firewall	M: Apreciable =4	Políticas de Controles Criptográfico	Uso de información cifrada para proteger información sensible, uso de firma digital, para la verificación de la autenticidad,	Evitar, Transferir y Asumir el Riesgo

Tabla 30. (Continuación)

Tipo de activo	Activo	Riesgos	Salvaguardas	Recomendación	Medidas
Soportes de Información	Disco Duro	A: Importante =9	Controles contra códigos maliciosos y respaldo de la información	Prohibición de software no autorizado, controles de detección de uso de códigos maliciosos, análisis de actualización de software, antivirus, copias de respaldos.	Dispersar y atomizar el riesgo
	Memoria USB	A: Importante =9	Controles contra códigos maliciosos y respaldo de la información	Prohibición de software no autorizado, controles de detección de uso de códigos maliciosos, análisis de actualización de software, antivirus.	Dispersar y atomizar el riesgo
Equipamiento Auxiliar	Sistema de alimentación Ininterrumpida	B: Bajo =1	Respaldo de la información	Mantener un cambio periódico de la UPS y una revisión constante de la planta eléctrica para su buen funcionamiento.	Dispersar y atomizar el riesgo

Tabla 30. (Continuación)

Tipo de activo	Activo	Riesgos	Salvaguardas	Recomendación	Medidas
Instalaciones	Cableado Estructurado	A: Importante =9	Control de redes	Establecer revisión física a ducteria y canalización, esto puede evitar interrupciones en el servicio por daño en el cableado	Evitar, Transferir y Asumir el Riesgo
	CPD	A: Importante = 9	Uso no previsto	Control de acceso físico	Evitar y Reducir el Riesgo.
	Caídas eléctricas	A: Importante = 9	Planes de contingencia (plantas, UPS de alto poder)	Identificar y conocer protocolos de seguridad física e industrial.	Evitar y Reducir el Riesgo.
Personal	Funcionarios de la Empresa	MA: Critico =12	Uso de la información secreta para la autenticación, capacitaciones	Mantengan la confidencialidad de la información secreta para la autenticación, asegurándose que no sea divulgada a ninguna otra parte incluida las personas autorizadas.	Evitar y Reducir el Riesgo

Fuente: El autor

10.4.5 Verificación de aplicabilidad de los objetivos de control y controles establecidos en la norma ISO/IEC 27002:2013

La verificación se basa en la declaración de aplicabilidad y los criterios descritos en la siguiente tabla:

Tabla 31. Criterios de aplicabilidad

Códigos	**Significado**
D	El control se documentó e implementó
MD	El Control se lleva a cabo, pero el proceso debe ser documentado a fin de garantizar la repetitividad del mismo y aminorar los riesgos.
RD	El control no cumple las normas y es necesario diseñarlo para cumplir con estas
PNP	El proceso no está implementado. (Control requerido, no documentado y no implementado)
NA (Not Aplicable)	El control no es aplicable para la entidad

Fuente: El autor

Tabla 32. Estado de adopción de los objetivos de control y controles de acuerdo con la norma ISO/IEC 27002:2013

Clausula	Sec	Objetivo de Control/Control	Criterios de aplicabilidad
5. Políticas de Seguridad	5,1	Políticas de Seguridad de la Información	
	5.1.1	Políticas para la seguridad de la información	PND
	5.1.2	Revisión de las políticas para la seguridad de la información	PND
6 Organización de la Seguridad de la Información	6,1	Organización Interna	
	6.1.1	Roles y responsabilidades para la seguridad de la Información	RD
	6.1.2	Separación de Deberes	RD
	6.1.3	Contacto con las Autoridades	PND
	6.1.4	Contacto con grupos de interés especial	PND
	6.1.5	Seguridad de la Información en la gestión de proyectos	PND
	6,2	Dispositivos Móviles y Teletrabajo	
	6.2.1	Política para Dispositivos Móviles	PND
	6.2.2	Teletrabajo	PND

Tabla 32. (Continuación)

Clausula	Sec	Objetivo de Control/Control	Criterios de aplicabilidad
7 Seguridad del Recurso Humano	7,1	Antes de Asumir el Empleo	
	7.1.1	Selección	PND
	7.1.2	Términos y condiciones del empleo	RD
	7,2	Durante el empleo	
	7.2.1	Responsabilidades de la Dirección	PND
	7.2.2	Toma de conciencia, educación y formación en Seguridad	PND
	7.2.3	Proceso Disciplinario	PND
	7,3	Terminación y cambio de Empleo	
	7.3.1	Terminación o cambio de responsabilidades de Empleo	PND
8 Gestión de Activos	8,1	Responsabilidad por los Activos	
	8.1.1	Inventario de Activos	RD
	8.1.2	Propiedad de los Activos	MD
	8.1.3	Uso aceptable de los activos	RD
	8.1.4	Devolución de Activos	PND
	8,2	Clasificación de la Información	
	8.2.1	Clasificación de la Información	MD
	8.2.2	Etiquetado de la Información	RD
	8.2.3	Manejo de Activos	PND
	8,3	Manejo de Medios	
	8.3.1	Gestión de medios removibles	PND
	8.3.2	Disposición de Medios	PND
	8.3.3	Transferencia de medios físicos	PND

Tabla 32. (Continuación)

Clausula	Sec	Objetivo de Control/Control	Criterios de aplicabilidad
9 Control de Acceso	9,1	Requisitos del Negocio para el control de acceso	
	9.1.1	Política del Control de Acceso	PND
	9.1.2	Acceso a redes y servicios de red	PND
	9,2	Gestión de acceso de Usuarios	
	9.2.1	Registro y cancelación de acceso de usuarios	PND
	9.2.2	Suministro de acceso de usuarios	PND
	9.2.3	Gestión de Derechos de acceso privilegiado	PND
	9.2.4	Gestión de la Información secreta de autenticación de los usuarios	PND
	9.2.5	Revisión de los derechos de acceso de los usuarios	PND
	9.2.6	Retiro o ajuste de los derechos de los usuarios	PND
	9,3	Responsabilidades de los usuarios	
	9.3.1	Uso de información de autenticación secreta	PND
	9,4	Control de acceso a sistemas y aplicaciones	
	9.4.1	Restricción de acceso a la información	PND
	9.4.2	Procesamiento de Ingreso Seguro	PND
	9.4.3	Sistema de Gestión de contraseñas	MD
	9.4.4	Uso de programas utilitarios privilegiados	MD
	9.4.5	Control de acceso a códigos fuente de programas	PND

Tabla 32. (Continuación)

Clausula	Sec	Objetivo de Control/Control	Criterios de aplicabilidad
10 Criptografía	10,1	Controles Criptográficos	
	10.1.1	Política sobre el uso de controles criptográficos	PND
	10.1.2	Gestión de la llaves	PND
11 Seguridad Física y del Entorno	11,1	Áreas Seguras	
	11.1.1	Perímetro de Seguridad Física	PND
	11.1.2	Controles de acceso Físicos	PND
	11.1.3	Seguridad de oficinas, recintos e instalaciones	PND
	11.1.4	Protección contra amenazas externas y ambientales	PND
	11.1.5	Trabajo en áreas seguras	MD
	11.1.6	Áreas de despacho y carga	PND
	11,2	Equipos	
	11.2.1	Ubicación y protección de los equipos	PND
	11.2.2	Servicios de suministro	MD
	11.2.3	Seguridad del cableado	PND
	11.2.4	Mantenimiento de equipos	MD
	11.2.5	Retiro de activos	PND
	11.2.6	Seguridad de equipos y activos fuera de las instalaciones	PND
	11.2.7	Disposición segura o reutilización de equipos	PND
	11.2.8	Equipo de usuario desatendido	MD
	11.2.9	Pantalla de escritorio limpio y pantalla limpia	MD

Tabla 32. (Continuación)

Clausula	Sec	Objetivo de Control/Control	Criterios de aplicabilidad
	12,1	Procedimientos operacionales y responsabilidades	
	12.1.1	Procedimientos de operación documentados	PND
	12.1.2	Gestión de cambios	PND
	12.1.3	Gestión de capacidad	PND
	12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	PND
	12,2	Protección contra códigos maliciosos	
	12.2.1	Controles contra códigos maliciosos	PND
	12,3	Copias de Respaldo	
	12.3.1	Respaldo de la Información	MD
	12,4	Registro y monitoreo	
	12.4.1	Registro de eventos	PND
12 Seguridad de las Operaciones	12.4.2	Protección de la Información de Registro	PND
	12.4.3	Registros del administrador y del operador	PND
	12.4.4	Sincronización de relojes	PND
	12,5	Control de Software Operacional	
	12.5.1	Instalación de software en sistemas operativos	PND
	12,6	Gestión de la Vulnerabilidad Técnica	
	12.6.1	Gestión de las Vulnerabilidades técnicas	PND
	12.6.2	Restricciones sobre la instalación de software	PND
	12,7	Consideraciones sobre auditorias de sistemas de Información	
	12.7.1	Controles de auditorías de sistemas de Información	PND

Tabla 32. (Continuación)

Clausula	Sec	Objetivo de Control/Control	Criterios de aplicabilidad
	13,1	Gestión de la seguridad de las redes	
	13.1.1	Controles de Redes	PND
	13.1.2	Seguridad de los servicios de Red	PND
	13.1.3	Separación de las Redes	PND
13 seguridad de las Comunicaciones	13,2	Transferencia de Información	
	13.2.1	Políticas y procedimientos de transferencia de Información	MD
	13.2.2	Acuerdos sobre transferencia de información	MD
	13.2.3	Mensajería Electrónica	PND
	13.2.4	Acuerdos de Confidencialidad o no divulgación	MD

Tabla 32. (Continuación)

Clausula	Sec	Objetivo de Control/Control	Criterios de aplicabilidad
	14,1	Requisitos de Seguridad de los Sistemas de Información	
	14.1.1	Análisis y especificación de requisitos de seguridad de la Información	PND
	14.1.2	Seguridad de servicios de aplicaciones en redes Publicas	PND
	14.1.3	Protección de los servicios de las aplicaciones transaccionales	MD
	14,2	Seguridad de los procesos de desarrollo y soporte	
	14.2.1	Política de desarrollo seguro	NA
14 Adquisición, Desarrollo y Mantenimiento de Sistemas	14.2.2	Procedimientos de control de cambios en sistemas	NA
	14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	NA
	14.2.4	Restricción en los cambios a los paquetes de software	NA
	14.2.5	Principios de construcción de sistemas seguros	NA
	14.2.6	Ambiente de desarrollo seguro	NA
	14.2.7	Desarrollo contratado externamente	NA
	14.2.8	Pruebas de seguridad en sistemas	NA
	14.2.9	Pruebas de aceptación de sistemas	NA
	14,3	Datos de Prueba	
	14.3.1	Protección de los datos de prueba	PND

Tabla 32. (Continuación)

Clausula	Sec	Objetivo de Control/Control	Criterios de aplicabilidad
15 Relación con los proveedores	15,1	Seguridad de la Información en la relación con los proveedores	
	15.1.1	Política de seguridad de la información para las relaciones con los proveedores	PND
	15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	PND
	15.1.3	Cadena de Suministro de tecnología de información y comunicaciones	PND
	15,2	Gestión de la prestación de servicios de proveedores	
	15.2.1	Seguimiento y revisión de los servicios de los proveedores	MD
	15.2.2	Gestión de cambios en los servicios de los proveedores	NA

Tabla 32. (Continuación)

Clausula	Sec	Objetivo de Control/Control	Criterios de aplicabilidad
	16,1	Gestión de incidentes y mejoras en la seguridad de la Información	
	16.1.1	Responsabilidades y procedimientos	PND
	16.1.2	Reporte de eventos de seguridad de la información	PND
16 Gestión de Incidentes de Seguridad de la Información	16.1.3	Reportes de debilidades de seguridad de la información	PND
	16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	PND
	16.1.5	Respuesta a incidentes de seguridad de la Información	PND
	16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la Información	MD
	16.1.7	Recolección de Evidencia	PND

Tabla 32. (Continuación)

Clausula	Sec	Objetivo de Control/Control	Criterios de aplicabilidad
17 Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio	17,1	Continuidad de Seguridad de la Información	
	17.1.1	Planificación de la continuidad de la seguridad de la Información	PND
	17.1.2	Implementación de la continuidad de la Seguridad de la Información	PND
	17.1.3	Verificación, revisión y evaluación de la continuidad de seguridad de la Información	PND
	17,2	Redundancias	
	17.2.1	Disponibilidad de instalaciones de procesamiento de información	PND

Tabla 32. (Continuación)

Clausula	Sec	Objetivo de Control/Control	Criterios de aplicabilidad
18 Cumplimiento	18,1	Cumplimiento de requisitos legales y contractuales	
	18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	PND
	18.1.2	Derechos de propiedad Intelectual	PND
	18.1.3	Protección de Registros	MD
	18.1.4	Privacidad y protección de información de datos personales	PND
	18.1.5	Reglamentación de Controles Criptográficos	PND
	18,2	Revisiones de Seguridad de la Información	
	18.2.1	Revisión Independiente de la Seguridad de la Información	PND
	18.2.2	Cumplimiento con las políticas y normas de seguridad	PND
	18.2.3	Revisión del cumplimiento técnico	PND

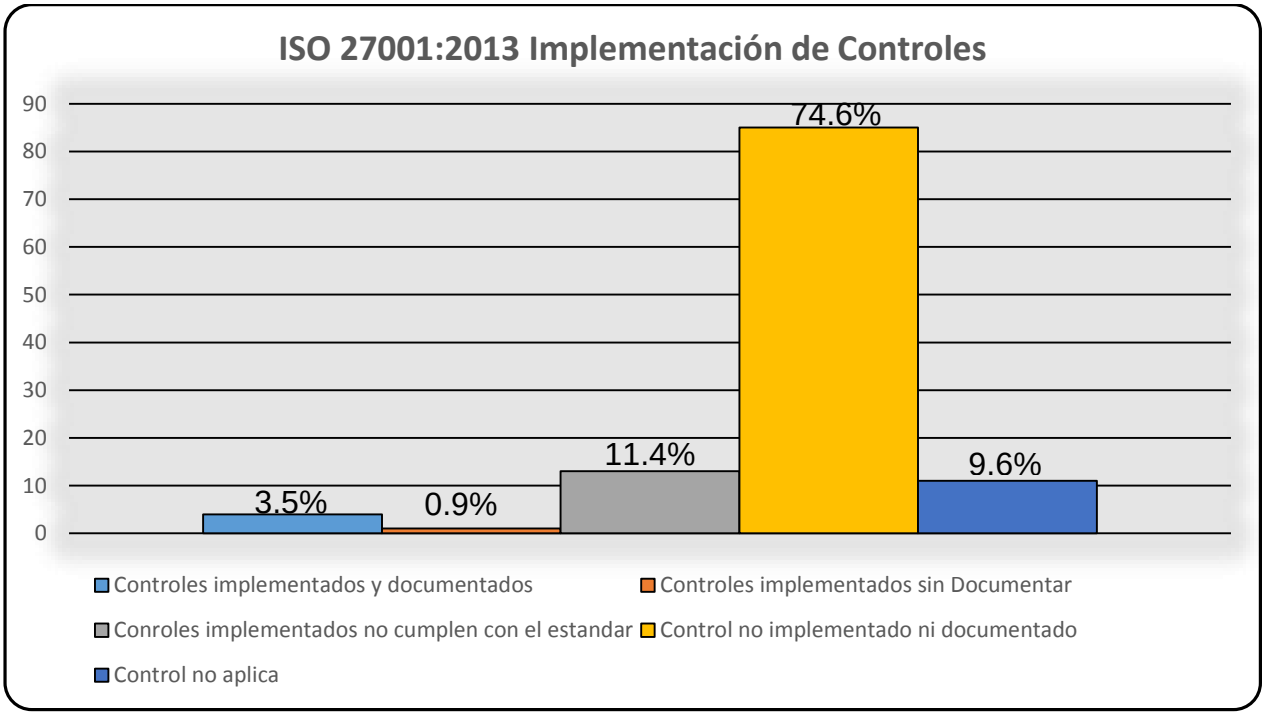
Fuente: El autor

Tabla 33. Resumen estado de adopción objetivos de control y controles

Cantidad	Códigos Status	Significado	Contribución %
4	D	El control se documentó e implementó	3,5%
1	MD	El Control se lleva a cabo, el proceso debe ser documentado a fin de garantizar la repetitividad del mismo y aminorar los riesgos.	0,9%
13	RD	El control no cumple las normas y es necesario diseñarlo para cumplir con estas	11,4%
85	PNP	El proceso no está implementado. (Control requerido, no documentado y no implementado)	74,6%
11	NA (Not Aplicable)	El control no es aplicable para la empresa	9,6%
114	TOTALES		100%

Fuente: El autor

Ilustración 28. Análisis estado de implementación



Fuente: El autor

De acuerdo con la gráfica anterior, los controles no se encuentran implementados ni documentados, por lo que se requiere el debido proceso con lo que se podrá garantizar lo dispuesto en el estándar ISO/IEC 27002:2013. El nivel de cumplimiento en este caso es bajo y representa para la entidad un grado Alto de riesgo. Es una alerta para que se dispongan los elementos necesarios y así convertirlo en un nivel bajo, razón por la cual es preciso rediseñarlos teniendo en cuenta los resultados del análisis de riesgos y los requerimientos de protección del bien informático, una vez con este control se lograra evitar grandes pérdidas de información y vulnerabilidades.

De acuerdo con lo analizado se logró evidenciar las falencias de UNISANAR IPS en cuanto a la aplicabilidad de los controles, por lo que se hace necesario desarrollar lo dispuesto en la norma, para evitar posibles ataques en los sistemas de información de la empresa.

10.4.6 Diseño

10.4.6.1 Políticas y objetivos de seguridad de las informaciones recomendadas a UNISANAR IPS. Con base a la evaluación de riesgos según la NTC-ISO/IEC 27001:2013 donde se establecen 14 dominios, para utilizar los controles de cada dominio como apoyo a la seguridad de la información debe tener en cuenta la entidad UNISANAR IPS lo siguiente:

10.4.6.2 *Alcance del SGSI.* En la planeación para la implementación de un SGSI es muy importante definir el alcance del sistema en UNISANAR IPS.

El alcance del Sistema de Gestión de Seguridad de la Información se limita temporalmente en la sede principal de UNISANAR IPS, la cual se encuentra ubicada en la ciudad de Quibdó, pues es allí, donde se toman las decisiones y se gestiona todo lo concerniente a la administración de la entidad, se le aplicara las políticas de los procesos tanto internos como externos a todo el personal de la entidad sin importante su situación contractual, área o jerarquía.

Objetivos del Sistema de Gestión de Seguridad de la información

10.4.6.3 Objetivos del SGSI. UNISANAR IPS en cumplimiento de su misión, visión y objetivos estratégicos establece los siguientes objetivos para el SGSI:

1. Ampliar y mantener la satisfacción de los clientes tanto internos como externos de UNISANAR IPS.
2. Aumentar el nivel competitivo de todos los funcionarios de UNISANAR IPS.
4. Certificar el acceso a la información acorde a los niveles y juicios de seguridad señalados por UNISANAR IPS y la normatividad aplicable.

5. Guardar la integridad de la información de UNISANAR IPS, circunscribiendo las exigencias de seguridad ajustables y los resultados de la evaluación y el tratamiento de los riesgos identificados.
6. Garantizar que la información esté disponible para los usuarios y procesos en el momento en que sea requerida.

Política del Sistema de Gestión de Seguridad de la Información

Acuerdos

Todos los funcionarios de UNISANAR IPS, se deben comprometer al correcto cumplimiento en los acuerdos de confidencialidad, donde los funcionarios no difunden la información de calidad reservada a la que tengan acceso, respetando la clasificación de la información, donde cualquier trasgresión a lo establecido se considera como una falta grave a la seguridad.

Uso de activos (Uso y Clasificación de la información)

La manipulación de la información física y digital de la empresa se clasifica de acuerdo con la competencia de cada área y los permisos otorgados para el manejo de la misma los cuales será de exclusividad de los jefes de cada dependencia y este a su vez informará sobre la actualización de los privilegios a los encargados con el fin de llevar el debido control y minimizar el uso o modificaciones no autorizada de la información de la empresa.

Conexión a la red

No se tendrá acceso a páginas interactivas como Facebook, YouTube, Skype, WhatsApp web, como a páginas relacionadas con pornografías, músicas, descarga de archivos, películas, video juegos, archivos ejecutables u otras similares, que

permitan el intercambio de información o que distraiga las actividades propias de la empresa y atenten contra la misma en cuanto a su confidencialidad, integridad y disponibilidad de la información. Todos los empleados son responsables del correcto y adecuado uso de esta herramienta.

Acceso a sistemas y aplicativos

Es de responsabilidad exclusiva del encargado del área informática la configuración de los equipos, como la sincronización de dispositivos controlando así examinará la copia o la extracción de dichos dispositivos.

Capacitación y educación en seguridad de la información

Al hacer parte de la empresa UNISAR IPS, se efectuará la respectiva inducción, de cada una de las políticas, procedimientos y normas con los que cuenta la entidad, conociendo así las obligaciones que se tiene y las sanciones pertinentes por el incumplimiento de las mismas, de igual forma se actualizara periódicamente sobre los cambios realizados.

Control de acceso

El acceso al cuarto de comunicaciones será restringido, el cual se le realizara un control de ingreso, sus equipos estarán protegidos y ubicado de acuerdo con los controles necesarios para mantener un ambiente idóneo, como el de la humedad y temperatura, inundaciones, eléctricos, y sus respectivos respaldos de acuerdo con lo establecido.

Control de software malicioso

Los archivos estarán protegidos mediante softwares antivirus licenciados, conservando siempre la última actualización, y parches de seguridad y mantendrá un conjunto de políticas, normas, estándares, procedimientos y guías que garanticen la mitigación de riesgos.

Copias de respaldo

Se establecerá copia de respaldo para asegurar que será recuperara la información después de algún tipo de falla, dándole un nivel apropiado de seguridad, protección y alcance para el momento de ser requerida, por lo que esta copia se hará de forma periódica generando información exacta y completa.

Control de acceso lógico

Los funcionarios que tengan usuario y contraseña institucional son responsables sobre el manejo y seguridad de la misma, para así preservar la confidencialidad de los datos.

Gestión de contraseñas

Se podrá permitir que las contraseña permita cambios por parte del usuario, siempre y cuando sean contraseñas de calidad, y con cambios de manera regular evitando el rehúso de estas las cuales cada que sean digitadas no se podrán observar en la pantalla, si existen olvido de la contraseña solo será reestablecida por el personal encargado. Es importante que las contraseñas sean creadas con letras, números y caracteres especiales.

Escritorio y pantalla limpia

Se debe guardar la información física en un sitio confiable y de acceso único, al estar inactivo los equipos se bloquearán la pantalla y el teclado, el cual se reactivará con la contraseña del usuario del equipo, al culminar la jornada laboral se deberá cerrar las aplicaciones en uso y apagar el equipo de cómputo.

Reporte e investigación de incidentes de seguridad de la información

Los funcionarios deberán reportar mediante formato previo de la entidad, cualquier tipo de acción requerida como violación de la seguridad de la información, el cual será atendido de manera inmediata por los encargados de la seguridad de la información con su respectivo monitoreo.

Terminación o cambio de empleo

Los funcionarios deberán mantener la confidencialidad y no difusión de la información clasificada de la empresa con el fin de protegerla, el cual continuara terminado el contrato por un periodo determinado.

11 RECOMENDACIÓN

Es indispensable que la Alta Gerencia acepte, entienda, apruebe y dé a conocer las políticas de seguridad de la información a toda la empresa, realizando así capacitaciones y mucha sensibilización a todos los que integran UNISANAR IPS, en el manejo de la seguridad y la importancia de los sistemas de información, para así lograr minimizar los posibles riesgos y amenazas a los que se puedan ver expuestos.

12 CONCLUSIONES

Los sistemas de información y las TIC juegan un papel muy importante en el servicio que le presta UNISANAR IPS, ya que con esto se logra sacar grandes ventajas competitivas manteniendo siempre los objetivos; sin embargo, los avances tecnológicos y su uso son de total desconocimiento por la alta gerencia lo que impide que se mantenga una implementación en el manejo de la seguridad de la información.

Se procede con el diagnostico que vive la organización en la actualidad con respecto a la seguridad del activo más importante, teniendo en cuenta la norma Técnica Colombiana ISO 27001:2013. Luego se efectúa el levantamiento de los activos de la información en UNISANAR IPS.

Se realiza la identificación, valoración y análisis de riesgos de acuerdo a la Metodología MAGERIT, lo que permite determinar los activos críticos de la entidad, el alto impacto que puede generar el quebrantamiento de un activo y la declaración del plan de tratamiento de riesgos en la prestación de servicios y funcionamiento dentro de los procesos de UNISANAR IPS, permitiendo que la alta dirección tenga un mejor entendimiento de la importancia de la infraestructura de las tecnologías de la información en el desarrollo normal de los procesos de la empresa y por ende en los objetivos misionales.

UNISANAR IPS en la realidad registra un nivel de riesgo informático importante, que con la colaboración de la alta gerencia y de todo el personal es viable contrarrestar.

Esta monografía permite a la entidad establecer procedimientos, construir controles y diseñar el plan de tratamiento de riesgos, asintiendo el nivel de cumplimiento del Sistema de Gestión de Seguridad de la Información de manera exitosa.

13 BIBLIOGRAFÍA

233003 Sistema de Gestión de seguridad de la información SGSI. Universidad Nacional Abierta y a Distancia. [En línea] 24 de 11 de 2014. http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/index.html

233003 Sistema de Gestión de seguridad de la información SGSI. Universidad Nacional Abierta y a Distancia. [En línea] 2013. http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/index.html

Alvarez Basaldua, L. D. *bib.uia.mx.* Seguridad en Informatica, Auditoria de Sistemas. [en línea] 2005. http://www.bib.uia.mx/tesis/pdf/014663/014663.pdf

Bisogno, M. V. *http://materias.fi.uba.ar/.* Metodología para el Aseguramiento de Entornos Informatizados" – MAEI. [en línea] 12 de Octubre de 2004. http://materias.fi.uba.ar/7500/bisogno-tesisdegradoingenieriainformatica

Briceño Sanz, F. J. *IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD EN UN EDIFICIO PÚBLICO.* [en línea] Octubre de 2010. orff.uc3m.es: http://orff.uc3m.es/bitstream/handle/10016/10587/PFC_FranciscoJavier_Briceno_Sanz.pdf?sequence=1

Buitrago Estrada, J. C., Bonilla Pineda, D. H., & Murillo Varon, C. E. *DISEÑO DE UNA METODOLOGIA PARA LA IMPLEMENTACIÓN DEL SISTEMA.* [En línea] 2012. http://repository.ean.edu.co/bitstream/handle/10882/2692/MurilloCarol2012.pdf?sequence=1

Collazos Balaguer, M. (s.f.). *La nueva versión ISO 27001:2013.* Colegio de Ingenieros del Perú. [En línea]. file:///D:/Documentos%20Usuario/Downloads/PRESENTACION_MANUEL_COLLAZOS_-_1.pdf (233003 Sistema de Gestión de seguridad de la información SGSI, 2013)

Custodia-documental.com. [En línea] 23 agosto, 2011. http://www.custodia-documental.com/familia-iso-27000-seguridad-de-la-informacion/

Familia ISO 27000: Seguridad de la Información. El blog de la gestión documental. [En línea] 23 de 08 de 2011. http://www.custodia-documental.com/familia-iso-27000-seguridad-de-la-informacion/

Gandini, I., Isaza, A., & Delgado, A. *Ley de Delitos Informaticos en Colombia*. [en línea] 13 de Diciembre de 2014. http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia

Hurtado Rubén, Rodríguez Wilson, Fuentes Héctor, Galleguillos Carlos. Impacto en los beneficios De la implementación de Las normas de calidad ISO 9000 en las empresas. [En línea] 2009. http://www.revistaingenieria.uda.cl/Publicaciones/230003.pdf

INTECO. Estándares de Gestión de la Seguridad de la Información. [en línea] 09 de Marzo de 2010. https://www.youtube.com/watch?v=vWAV0bdWvtI

INTECO. Implantación de un SGSI. [en línea] 22 de Marzo de 2010. https://www.youtube.com/watch?v=i_3z68QGaJs

ISMS Forum Spain. (s.f.). Obtenido de Protege tu Informacion. [En línea] http://www.protegetuinformacion.com/perfil_tema.php?id_perfil=6&id_tema=60

ISO 27001:2013 Un cambio en la integración de los sistemas de gestión. SGSI Blog especializado en Sistemas de Gestión. [En línea] 24 de 11 de 2014. http://www.pmg-ssi.com/2014/11/iso-270012015-un-cambio-en-la-integracion-de-los-sistemas-de-gestion/

kioskea.net. [En línea] http://es.kioskea.net/faq/4739-como-proteger-su-empresa-riesgos-y-recomendaciones

Kosutic, D. (s.f.). *¿Qué es norma ISO 27001?* 27001 Academy [En línea] http://advisera.com/27001academy/es/que-es-iso-27001/

López, A., & Ruiz, J. ISO27000. El portal de ISO 27001 en Español. [En línea] 2005. http://www. iso27000. es/iso27000. html.

NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001. Icontec. [En línea] 13 de Diciembre de 2014. http://www.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

ordenador.wingwit. (s.f.). Computer Informacion. [En línea]. http://ordenador.wingwit.com/Redes/network-security/75816.html#.VEE3APmG9JM

Poveda, José M. ISO 27001. [En línea] Marzo de 2011. https://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-8.pdf.

Rodriguez, J. *Tecnologia Pyme*. [En línea] 05 de Febrero de 2013. http://www.tecnologiapyme.com/productividad/ventajas-al-usar-un-dispositivo-de-proteccion-firewall-en-la-red-de-la-empresa

Tiposde.org. (s.f.). Tipos de Firewall. [En línea] http://www.tiposde.org/informatica/636-tipos-de-firewall/

Vargas, Ana C., Castro M., Alonso. Sistemas de Gestión de Seguridad de la Información. [En línea]. http://archivo.ucr.ac.cr/docum/ISOEIC27000.pdf

14 ANEXOS

Anexo A. Entrevista a los funcionarios UNISANAR IPS

El siguiente cuestionario tiene como fin demostrar que tanto conocen sobre la seguridad informática y lo que comprende.

Seguridad General

1. ¿De cuántos ordenadores dispone UNISANAR IPS?

1-5 5-10 +10

2. Los equipos de cómputo de la entidad, ¿tienen instalado antivirus?

Sí No No se

3. El antivirus que tienen instalado (si es el caso), ¿está actualizado con las últimas definiciones?

Sí No No se

4. ¿Se realiza un mantenimiento informático periódico sobre los ordenadores de la empresa?

Sí No No se

5. ¿Se utilizan programas de descarga de archivos de usuario (música, películas, programas...)?

Sí *No* *No se*

6. ¿Conoce si UNISANAR IPS cuenta con un servidor central de datos?

Sí No No se

7. Sobre dicho servidor, ¿sabe si se le realiza un mantenimiento informático periódico?

Sí No No se

Comunicaciones

8. ¿En la entidad se trabaja desde algún ordenador externo, por conexión vía Internet?

Sí No No se

9. Si la conexión en UNISANAR IPS es mediante la red (WIFI), ¿conoce si se utilizan las medidas de seguridad pertinentes para proteger dicha conexión?

Sí No No se

Datos de la empresa

10. ¿Los computadores de la entidad tienen datos de la empresa almacenados en el disco duro?

Sí No No se

11. ¿Se realiza copia de seguridad de la información que maneja la entidad?

Sí No No se

12. ¿Con qué frecuencia?

Diario semanal Mensual

13. ¿Usted o sus colaboradores a cargo poseen alguna copia de seguridad (USB / DVD / Otro) fuera de la empresa?

Sí No No se

14. ¿Se realiza un mantenimiento de las copias de seguridad de UNISANAR IPS?

Sí No No se

Programas y Aplicaciones Informáticas

15. ¿Los programas y aplicaciones usadas en UNISANAR IPS, cumplen con las características de seguridad informática?

Sí No No se

16. ¿Hay algún encargado de instalar/desinstalar los programas y aplicaciones informáticas en UNISANAR IPS?

Sí No No se

Seguridad Informática

17. ¿Conoce usted algo referente a la seguridad informática?

Sí No No se

18. ¿Qué sabe al respecto?

19. ¿La compañía ha dispuesto políticas de seguridad para el manejo de las herramientas informáticas de las que disponen para la gestión de su proceso?

Sí No No se

- ¿Cuáles?
-

20. ¿Qué medidas de seguridad toma para proteger la información de UNISANAR IPS?

Anexo B. Carta de Compromiso UNISANAR IPS

1. Que se informa de las leyes nacionales e internacionales de derechos de autor que regulan el uso de soportes lógicos (Software).

2. Que se informa sobre el aval que requiere cualquier instalación de software en los equipos de la empresa por parte del Sistemas y que solo las personas de Soporte Técnico pueden instalarlo.

3. Que las personas de Soporte Técnico, son las únicas habilitadas para realizar mantenimiento preventivo y correctivo de los computadores institucionales.

4. Que se dio a conocer sobre la prohibición del uso de programas o recursos para los cuales no exista una licencia o autorización de uso valido a nombre de la empresa.

5. Que se dio a conocer sobre la prohibición de instalar software para descargar música, videos u otras actividades ajenas al objeto y misión de la empresa.

6. Que se prohíbe la copia y/o distribución de software adquirido por la empresa a terceros.

7. Que cualquier acto que infrinja las normas sobre derechos de autor o implique el uso indebido de una licencia, compromete personalmente exclusivamente a quien este responsable del equipo, quien lo haría sin el aval de la empresa, eximiéndola así de cualquier responsabilidad.

8. Que se prohíbe la modificación de las configuraciones y funciones de los elementos de protección y seguridad del equipo o del software.

9. Que se me prohíbe alterar el hardware y/o software del equipo de forma parcial o completa.

10. Que los elementos entregados en los puestos de trabajo (cables, parlantes, tarjetas, controles, mouse) son uso exclusivo de la institución y se deben dejar en el sitio donde se encontraron.

_____	_____
Representante Legal	Área De Sistemas
UNISANAR IPS	UNISANAR IPS%