**ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL**


**Facultad de Ingeniería en Electricidad y Computación**

# "ANÁLISIS, DISEÑO E IMPLEMENTACIÓN DE UN PLAN DE SEGURIDAD INFORMÁTICA CON BASE EN LA NORMA ISO/IEC 27018:2014 PARA UNA EMPRESA QUE OFRECE SOFTWARE COMO SERVICIO (SAAS)"

**TRABAJO DE TITULACIÓN**

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

**Presentado por:**

**ANGEL PATRICIO AGUIRRE SANABRIA**

GUAYAQUIL - ECUADOR

2019

# AGRADECIMIENTO

Gracias a Dios por permitirme tener y disfrutar a mis seres queridos, a ellos por apoyarme en cada proyecto de mi vida. A todos quienes permitieron que esté proyecto sea posible, maestros que compartieron sus conocimientos, amigos que están ahí con palabras de apoyo.

# DEDICATORIA

Este trabajo está dedicado a Dios, a mis seres queridos que han hecho posible que pueda avanzar en mi área profesional y que han estado ahí siempre con palabras de aliento.

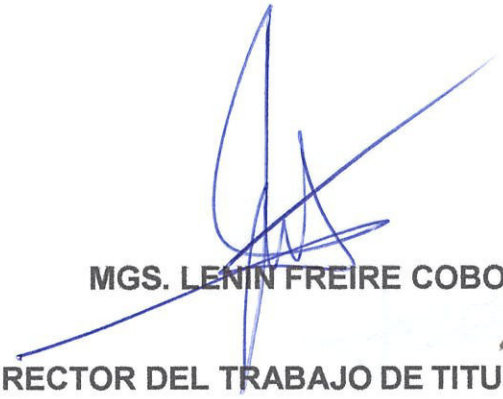
A mis padres que siempre me han brindado su apoyo incondicional y me han inculcado el seguir mejorando día a día.

A mis maestros porque gracias a los conocimientos impartidos en las jornadas de clases pude sacar adelante este proyecto y muchos otros a nivel profesional.

# TRIBUNAL DE SUSTENTACIÓN

**MGS. LENIN FREIRE COBO**

**DIRECTOR MSIG/MSIA**



**MGS. LENIN FREIRE COBO**

**DIRECTOR DEL TRABAJO DE TITULACIÓN**

**MGS. OMAR MALDONADO DAÑIN**

**MIEMBRO DEL TRIBUNAL**

# DECLARACIÓN EXPRESA

"La responsabilidad del contenido de este Trabajo de Titulación, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral"

(Reglamento de exámenes y títulos profesionales de la ESPOL)

**ANGEL PATRICIO AGUIRRE SANABRIA**

# RESUMEN

El presente proyecto trata de cubrir la información referente al desarrollo de las Tecnologías de la Información hacia el uso de Computación en la Nube, el mismo que ha tenido un crecimiento importante en los últimos años gracias a los beneficios de los servicios ofrecidos.

Se pretende con el presente documento incluir conceptos básicos para el entendimiento de este nuevo modelo de servicios con el propósito de brindar información a profesionales del área así como a cualquiera que le sea de interés el tema.

Se incluye un breve Análisis de las normas ISO así como el cumplimiento normativo necesario para la implementación de Computación en la Nube profundizando en la parte que se refiere a la Seguridad de la información en la Nube.

Finalmente, la idea es aportar con aspectos positivos para que las empresas vean con mayor confianza a este nuevo modelo de Servicios.

# ÍNDICE GENERAL

# ÍNDICE DE FIGURAS

# ÍNDICE DE TABLAS

# INTRODUCCIÓN

El término “nube” empezó a utilizarse en los 90’s de forma limitada, siendo la empresa Salesforce.com uno de los primeros en introducir el concepto de Software como Servicio al entregar aplicaciones para empresas por medio de un sitio web en 1999. Luego de tres años en el 2002 la empresa Amazon al modernizar sus Centros de Datos inicio la entrega de Computación en la Nube a clientes externos, servicio que se conoce como Amazon Web Service (AWS).

Google en el 2006 lleva la Computación en la Nube hacia los usuarios comunes y corrientes con su servicio de Google Docs, lo que permitió a los internautas comenzar a disfrutar de este tipo de servicios que luego han ido en aumento por parte de diferentes empresas; y es así como hoy en día la nube permite realizar tareas cotidianas como editar documentos, fotos, ver videos, jugar, etc., servicios a los cuales se puede acceder desde cualquier parte siendo requerimiento básico la conectividad a Internet.

Los modelos de servicios en la nube han permitido que las pequeñas y medianas empresas puedan ser mucho más competitivas porque pueden acceder al uso de software contable o de facturación a través de planes sin

tener que preocuparse por el alto costo en equipos, licenciamiento y dedicarse exclusivamente a su modelo de negocio.

Sin embargo y a pesar de que el uso de servicios en la nube tiene un vertiginoso ascenso existen quienes aún no tienen la plena confianza y mencionan sus preocupaciones en cuanto a la seguridad y privacidad debido a que se tiene la percepción de pérdida de control de su información. El elegir un proveedor de servicios en la nube debe ser una decisión responsable y en la cual debe prestarse total atención a los términos y condiciones del contrato.

Para mejorar la confianza que se tiene en un proveedor de servicios en la nube, en el 2014 la ISO/IEC publicó la Norma ISO/IEC 27018:2014 la cual se suma a otras normas sobre Seguridad y cuyo objetivo es brindar una guía para la implementación de controles para los servicios en la nube. La norma ISO/IEC 27018 está basada en leyes y regulaciones emitidas por la unión Europea convirtiéndose en el primer estándar internacional sobre privacidad en la nube.

El presente trabajo realizará un Análisis de los Controles de esta norma diseñando un Plan de Seguridad basada en el acceso lógico a una solución ERP que es ofrecida como Software como Servicio (SaaS) por una empresa desarrolladora de software Ecuatoriana con el fin de mejorar la confianza de los clientes sabiendo que el proveedor de los servicios adopta medidas en lo que se refiere a la protección de los datos.

# CAPÍTULO 1

## GENERALIDADES

### 1.1 Antecedentes

Los servicios en la nube han experimentado un rápido crecimiento desde el 2012 en el que se estimaba el gasto en más de 111 billones hasta el 2017 en el que la facturación sobrepasa los 200 billones de dólares; esto ha permitido que la Nube avance de su etapa inicial a una etapa de madurez en la cual los proveedores de los servicios han invertido importantes recursos en mejorar sus sistemas con medidas de vanguardia para mejorar la seguridad y privacidad en cuanto a la protección de los datos.

Por el año 2012 la Comisión Europea llegó a identificar la ausencia de un marco internacional auditable para la parte que corresponde al procesamiento de datos personales de parte de los proveedores de servicios en la nube, considerándose esto como un obstáculo clave al querer adoptar la computación en la nube. Como parte de una pronta respuesta de la ISO/IEC empezó a trabajar en la elaboración de un estándar para la nube que involucre el procesamiento de datos personales, considerando los ya existentes estándares de Seguridad de la Información como lo son el ISO/IEC 27001 e ISO/IEC 27002.

Publicada en el año 2013 la norma ISO/IEC 27018 está centrada en la protección de los datos personales en la nube, la misma especifica mínimas medidas de seguridad que deben adoptarse por parte de los proveedores de la nube incluyendo controles de cifrado y acceso. La finalidad de la norma ISO/IEC 27018 es proporcionar una base práctica que induzca la confianza en la industria de la nube; sirviendo también a las empresas que brindan el servicio que cuenten con una orientación clara para cubrir los temas legales y regulatorios de sus clientes.

## 1.2 Descripción del Problema

Hasta antes de la llegada de la Norma ISO/IEC 27018:2014 los proveedores que manejan procesos de tratamiento de datos sólo podían certificarse en cuanto a las normas UNE-ISO/IEC 27001:2014 [1] en la cual el sistema es muy flexible en cuanto a establecer un Sistema de Gestión de Seguridad de la Información (SGSI) que identificaba riesgos generales y la privacidad seguía siendo una incógnita ya que no había parámetros internacionalmente reconocidos.

El software como servicio (SaaS) provee una característica que lo hace especial frente a otras opciones y es que no requiere ninguna instalación en equipos físicos en las instalaciones de la empresa que lo contrata; al mismo tiempo esta característica que lo destaca es uno de sus problemas principales ya que al estar ejecutándose en servidores remotos pone en alerta la percepción de seguridad en cuanto al tema de acceso físico y lógico.

En lo concerniente a la plataforma ERP de una empresa Ecuatoriana desarrolladora de software y en su acceso lógico, la cual funciona bajo la modalidad de Software como Servicio (SaaS) la misma no es ajena a este problema que posee el tipo de servicio por lo que se debe buscar una pronta solución para mejorar esa percepción de seguridad y brindar

tranquilidad a todas las empresas que hoy en día lo utilizan como una de sus principales herramientas de trabajo.

Si bien es cierto que el servicio no ha sufrido de incidentes deben considerarse riesgos de accesos indebidos como por ejemplo la utilización de usuarios y claves que ya no laboren en la empresa o el uso de credenciales de usuarios que se encuentren de vacaciones cuyos efectos pueden llevar a la pérdida, alteración, destrucción o divulgación de los datos que contienen información financiera, de clientes y proveedores.

Debido a que no existe una política de seguridad es necesaria la implementación de un Sistema de Gestión de Seguridad para el ERP de la empresa ecuatoriana desarrolladora del software a partir de la norma ISO/IEC 27018:2014 que disminuya o mitigue los riesgos de acceso lógico a la información de sus clientes.

## 1.3 Solución Propuesta

Con la norma ISO/IEC 27018:2014 el panorama en cuanto a la privacidad de los datos cambia sustancialmente debido a que los clientes de los servicios en la nube junto a las autoridades reguladoras ya pueden conocer

si el proveedor que brinda el servicio ha acogido medidas en cuanto a la protección de los datos lo cual también es auditable y verificable por un tercero.

La solución propuesta en cuanto a mejorar el acceso lógico a la aplicación ERP se basa en la elaboración de Políticas de Seguridad en base al Dominio de Control de Accesos definido en la Norma ISO/IEC 27018:2014, la cual es el primer estándar internacional que se centra en la privacidad de la información en la nube.

Para mejorar la seguridad de la información se deben establecer políticas para que tanto el personal del proveedor así como algún subcontratista si lo hubiere deben estar vinculados a acuerdos de confidencialidad y accedan a los datos mediante operaciones de autenticación y acceso.

Los beneficios que se esperan lograr con la aplicación de estos Controles es que el acceso lógico a la plataforma se realice bajo las medidas adoptadas por el proveedor del Servicio en cuanto a la protección de los datos lo que también a su vez se convierte en una ventaja competitiva para la plataforma y mejora su posición frente a la competencia otorgando al

cliente un nivel de seguridad mayor al que brindan otras empresas. Además se ofrecerá capacitación en cuanto a la Seguridad Informática orientada al Control de acceso a la aplicación ERP a los clientes como beneficio adicional incluido en las actualizaciones periódicas que se realizan de la aplicación.

## 1.4 Objetivo General

Analizar, Diseñar e Implementar la norma ISO/IEC 27018:2014 para una empresa que ofrece Software como Servicio (SaaS) a través de Políticas de Seguridad basadas en los Controles de Acceso Lógico.

## 1.5 Objetivos Específicos

- Introducir el estado actual de soluciones de Software como Servicio (SaaS) en nuestro medio.
- Analizar la norma ISO/IEC 27018:2014 a través del Marco Teórico.
- Realizar un correcto levantamiento de información de la solución de ERP en la nube.
- Analizar y Diseñar un Plan de Seguridad Informática a partir de las indicaciones de la norma ISO/IEC 27018:2014 enfocadas al Control de Acceso Lógico.

- Implementar controles y guías incluidos en los Estándares Internacionales para protección de la Información de Identificación personal (PII).
- Aportar confianza a través de la realización de políticas de seguridad con el fin de mejorar el control de acceso a la aplicación tanto a nivel proveedor como cliente.

## 1.6 Metodología

La metodología en la cual estará basado el presente documento estará regida por la referencia del proceso de implementación de un SGSI basado en ISO/IEC 27001 para la nube. Los controles para el Plan de Seguridad toman las directrices específicas de la norma ISO/IEC 27018:2014 los cuales fueron creados inspirados en la ISO/IEC 27002 [2].

# CAPÍTULO 2

## Marco Teórico

### 2.1 Seguridad de la Información

La Seguridad de la Información debe cumplir con la finalidad de resguardar los datos importantes de las empresas, instituciones u organizaciones. Es común confundir los términos seguridad de la información con seguridad informática ya que parecen conceptos iguales pero no son lo mismo.

La Seguridad de la información es mencionada como el plan de acción para la evaluación de amenazas y minimización de los riesgos bajo el uso de normativas o de buenas prácticas [3].

La Seguridad Informática en cambio se centra en las implementaciones o soluciones técnicas que protegen la información a través del uso de antivirus, firewalls, entre otros. La Seguridad informática forma parte de la Seguridad de la Información.

Con el fin de entender mejor la Seguridad de la información definiremos 3 características claves de la misma:

- **Confidencialidad:** es la propiedad que permite prevenir la divulgación de la información a personas o sistemas que no estén autorizados. **Integridad:** es aquella característica que busca mantener a los datos libres de cualquier modificación no autorizada.
- **Disponibilidad:** es la característica que permite acceder a la información por parte de quienes deben acceder a ella.

## 2.2 Computación en la Nube

La Computación en la Nube consiste en la entrega de Servicios Informáticos bajo demanda como lo son servidores, base de datos, almacenamiento, aplicaciones, entre otros recursos TI a través de Internet.

**Beneficios de la Computación en la Nube**

- Eliminación de gastos excesivos en Centro de Datos, Servidores y su licenciamiento así como en la electricidad necesaria para su funcionamiento.
- Ejecución de grandes cantidades de recursos informáticos en cuestión de minutos.
- Escalamiento de los recursos de TI de forma Global a través de múltiples regiones alrededor del mundo.
- Mejora de la productividad del personal de TI.
- Actualización constante de los equipos ubicados en los Centros de Datos del Proveedor.
- Continuidad del negocio a través de las copias de seguridad y recuperación ante desastres.

## 2.3 Modelos de Servicio y Despliegue de Computación en la Nube

La Computación en la Nube está basada en tres modelos, los cuales son:

- **El Modelo de Consumo:** es aquel que ofrece una forma de consumo de cómputo y recursos de almacenamiento.
- **El Modelo de Servicios:** es un modelo muy conocido y que se ha desarrollado brindando tres servicios, los cuales son: servicio de infraestructura, servicio de plataforma y servicio de aplicación.

- **Infraestructura como Servicio (IaaS):** este servicio ayuda a evitar los gastos y la complejidad que puede significar la compra o administración de un centro de datos.

El aprovisionamiento y administración a través de Internet de éste tipo de Infraestructura puede escalar rápidamente hacia arriba o abajo según la demanda lo amerite debido a que los recursos de la nube son virtuales y el pago se realiza sólo por lo que se usa.


**Figura 2.1: Infraestructura como Servicio (IaaS)**

Los escenarios de negocios más comunes en los que se implementa IaaS en relación a la Figura 2.1, son los siguientes:

- Ambientes de Desarrollo y Prueba.
- Alojamiento de sitios web.
- Almacenamiento, Copias de seguridad y Recuperación.
- Aplicaciones Web.

- Computación de alto rendimiento.
- Análisis de Big Data.

**Ventajas de IaaS**

- Se eliminan los gastos iniciales de configuración y administración de un centro de datos in situ.
- Con IaaS se puede mejorar la continuidad del negocio y recuperación de desastres debido a que provee niveles de servicio correctamente especificados.
- Respuesta de forma rápida para ampliar los recursos en determinados picos de una aplicación y luego volver a disminuirlos para ahorrar costos.
- Se logra una mayor estabilidad, fiabilidad y compatibilidad al no ser necesario actualizar el software o hardware debido a que el proveedor del servicio asegura que la infraestructura sea confiable y cumpla con los SLAs.
- La seguridad para las aplicaciones y datos tiende a ser mejor que la que se puede lograr internamente.

- **Plataforma como Servicio (PaaS):** al igual que IaaS incluye servidores, almacenamiento y redes y añade un entorno completo de

desarrollo e implementación en la nube entregando desde simples aplicaciones hasta sofisticadas aplicaciones empresariales habilitadas para la nube. PaaS ha sido diseñado para admitir el ciclo de vida completo de una aplicación web desde la creación, la prueba, implementación, administración hasta la actualización manteniendo el esquema de compra de recursos según la necesidad con el pago sólo por el uso.

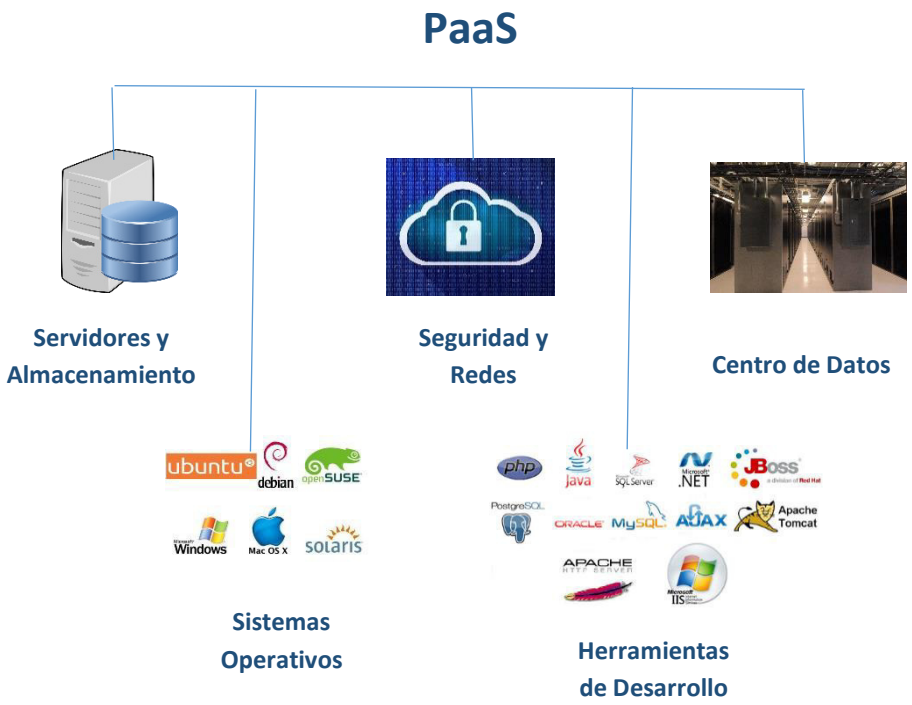



**Figura 2.2: Plataforma como Servicio (PaaS)**

Los escenarios más comunes de uso de PaaS son:

- Marco de desarrollo.

- Analítica o Inteligencia de Negocios.

**Ventajas de PaaS**

- Reducir el tiempo de codificación.
- Nuevas capacidades de desarrollo.
- Desarrollo para múltiples plataformas.
- Herramientas sofisticadas de forma asequible.
- Trabajo de equipos distribuidos geográficamente.
- Gestión del ciclo de vida de las aplicaciones.

- **Software como Servicio (SaaS):** como modelo de servicio permite a los usuarios usar aplicaciones basadas en la nube a través de internet; como por ejemplo el correo electrónico, software de oficina.


**Figura 2.3: Software como Servicio (SaaS)**

### Escenarios comunes donde se utiliza SaaS

Entre los escenarios comunes en los cuales se encuentra implementado SaaS (Software como Servicio) está el servicio de correo electrónico basado en la web, pueden ser de uso personal o empresarial. También se pueden alquilar aplicaciones de productividad, empresariales como la gestión de relaciones con los clientes (CRM), planificación de recursos empresariales (ERP) y la gestión de documentos.

**Ventajas de SaaS**

- Acceso a aplicaciones sofisticadas.
- Pago solo por uso.
- Uso de cliente gratuito.
- Movilidad de la fuerza de trabajo.

- **El Modelo de Implementación:** es el modelo que ofrece mayor flexibilidad, en él podemos encontrar varia maneras de implementar y utilizar la Nube.

**Nube Pública:** son aquellas operadas por proveedores de servicios en la nube, quienes le permiten al cliente el uso de sus recursos informáticos como servidores y almacenamiento. El cliente accede a través del navegador obteniendo organización, control y transparencia bajos pero si consigue prestaciones altas por parte del servicio.


**Figura 2.4: Nube Pública**

**Nube Privada:** en este tipo de nubes los recursos son aprovechados sólo por una organización, quien es la dueña de las instalaciones donde se aloja. En algunos casos las organizaciones les pagan a los proveedores de servicio para alojar en su centro de datos una nube privada, entre las mayores ventajas es poder conseguir mayor transparencia y control que en una nube pública.

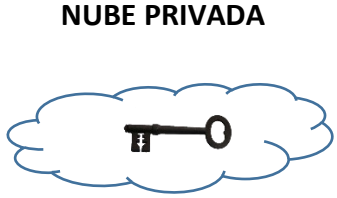



**Figura 2.5: Nube Privada**

**Nube Híbrida:** este tipo de nube combina las nubes públicas y privadas para permitirle a la organización compartir datos o aplicaciones, debido a que permite que este tipo de información se mueva entre ellas. Con esto las organizaciones logran alcanzar una mayor flexibilidad en cuanto al consumo de sus recursos informáticos y mejoras en sus implementaciones.

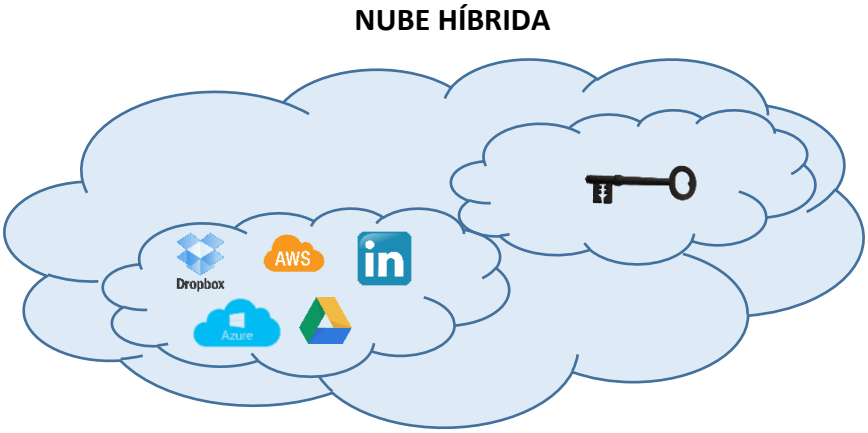



**Figura 2.6: Nube Hibrida**

## 2.4 Conceptos acerca de Riesgos

Los conceptos de los términos utilizados en el desarrollo se detallan a continuación [4]:

- **Información:** se conoce como un conjunto organizado de datos procesados los cuales constituyen un mensaje.
- **Activo:** son bienes y derechos adquiridos y controlados por una empresa con la finalidad de obtener beneficios.
- **Activo de Información:** son bienes que contienen información, utilizados por las empresas para funcionar y conseguir los objetivos propuestos, los cuales deben protegerse frente a cualquier riesgo o amenaza.
- **Identificación de Activo:** proceso en el cual se define y valora los activos a través de métricas de valoración.

- **Riesgo:** posibilidad de daño frente a determinadas circunstancias.
- **Riesgo Informático:** posibilidad de daño frente a amenazas que pueden atentar contra la seguridad de la información de una empresa [5].
- **Identificación de Riesgo:** reconocer los sucesos que se pueden producir en una empresa así como las consecuencias.
- **Impacto:** consecuencia efectiva que proyectará un efecto positivo o negativo sobre un determinado tratamiento de datos.
- **Probabilidad:** es la medida de que un determinado hecho suceda.
- **Vulnerabilidad Informática:** es una debilidad o fallo en un sistema operativo software o sistema que pone en riesgo la seguridad de la información.
- **Normas ISO:** son un conjunto de reglas orientadas a mejorar la gestión de una empresa aportándoles un valor agregado.
- **Norma ISO 27001:** es considerada la norma principal y permite conocer los requisitos para el sistema de gestión de seguridad de la información [6].
- **Norma ISO 27002:** la norma fue desarrollada para ser una guía de buenas prácticas describiendo controles recomendables en cuanto a la Seguridad de la Información.
- **Norma ISO 27018:** está centrada en la protección de los datos para servicios en la nube. Su finalidad es brindar confianza a los usuarios de

la nube en sus proveedores de servicios de que han implementado medidas de seguridad como controles de cifrado y acceso.

- **Política de Seguridad de la Información:** es un documento que denota buenas prácticas así como el compromiso con la seguridad de la información por parte de una empresa [7].

# CAPÍTULO 3

## Levantamiento de Información de la solución ERP en la nube con la cual se evaluará la norma ISO 27018:2014

### 3.1 Soluciones ERP en la nube del mercado en la actualidad

En la actualidad la mayoría de empresas buscan tener un sistema ERP para sus compañías, pero antes de mencionar a los más conocidos en el mercado es necesario describir conceptos generales que nos permitan entender mejor el funcionamiento y uso adecuado de los mismos.

**Definición de un ERP**: un Enterprise Resource Planning o “Sistema de Planificación de Recursos Empresariales” son aquellos programas destinados a hacerse cargo de las distintas operaciones internas de un empresa, las cuales van desde la producción, inventario, distribución, contabilidad, finanzas o incluso recursos humanos.

Un ERP supone una gran inversión por parte de la empresa pero luego de su implementación se produce una optimización en la gestión de los procesos maximizando la capacidad operativa de la empresa logrando un aumento de productividad.

### 3.1.1 Empresas desarrolladoras de ERP

La oferta de Software ERPs (Sistemas de Planificación de Recursos Empresariales) por parte de empresas que se dedican al desarrollo de soluciones continúa en aumento, más aun con la llegada de la nube sin embargo las empresas consideradas gigantes mantienen el control del mercado ya que brindan soluciones para diferentes sectores de actividades como se aprecia en la siguiente tabla:

**Tabla 1: Comparativa de fabricantes de ERP por Sector**

| Sector | SAP | Oracle | Microsoft | Epicor | Infor | CDC | NetSuite |
|---|---|---|---|---|---|---|---|
| Aeroespacial y Defensa | X | X | | X | X | | |
| Agricultura | X | X | | | | | X |
| Química | X | X | X | X | X | X | |
| Construcción | X | X | X | | X | X | |
| Ingeniería | X | X | X | | X | | |
| Servicios Financieros | X | X | X | X | X | X | |
| Publico | X | X | X | X | X | X | |
| Alimentario | X | X | X | | X | X | |
| Electrónica | X | X | X | X | X | | X |
| Equipamiento Industrial y Maquinaria | X | X | X | X | X | | |
| Productos Industriales | X | X | | | X | | |
| Farmacéuticas | X | X | X | X | X | X | X |
| Plástico | X | X | X | X | X | X | |
| Inmobiliario | X | X | X | | | X | |
| Venta minorista | X | X | X | X | X | X | X |
| Telecomunicaciones | X | X | X | | X | | X |
| Distribución Mayorista de bienes perecederos | X | X | X | X | X | X | X |
| Distribución mayorista de bienes no perecederos | X | X | X | X | | | |

**Fuente**: Panorama Consulting Solutions

De acuerdo a la tabla vista anteriormente se observa que los ERP de Microsoft, SAP y Oracle cubren casi en su totalidad los sectores por actividad indicados; basado en un reporte de Panorama Consulting Solutions de años anteriores dichas empresas cubrían el 56% del total de la demanda.

Hoy en día con el futuro enfocado en la nube y la movilidad, es lógico que las empresas se planteen dar el gran salto de sus Sistemas Informáticos Empresariales hacia la “en la Nube”; para saber si la empresa está realmente preparada se deben considerar los siguientes aspectos [8]:

- **Adaptación al cambio:** si la empresa tiene una escasa capacidad de adaptación al cambio no es recomendable llevar los procesos empresariales a la nube debido a que los empleados no están preparados para afrontar un cambio. Es mejor llevar a cabo cambios pequeños de aplicaciones en la nube como lo son módulos de gestión de documentos o incluso recursos humanos.
- **Seguridad:** es de los temas más controvertidos, se vuelve todo un reto convencer al mercado de que la seguridad que se brinda es real debido a que la compañía al perder el control físico sobre

los datos y aplicaciones se le dificulta asimilar la integración de la nube.

- **Control:** al formar parte de la nube, cada compañía debe tener muy claro que el control sobre los cambios, mantenimientos o cualquier actualización se perderá; esto debido a que el proveedor provee como parte de su servicio los mantenimientos y mejoras.
- **Arquitectura de la Organización:** para aprovechar las funcionalidades de la nube la inversión en hardware es pequeña, pero lo necesario si es una buena conexión a internet con la cual se pueda explotar todo el potencial. El limitante para aquellas compañías que tienen sucursales en ciudades más pequeñas es el limitado acceso a un ancho de banda adecuado.
- **Organización:** aquellas compañías con toda su infraestructura on-premises (en sitio local) y que cuentan con un departamento de sistemas numeroso, encargados de realizar los mantenimientos y mejoras de su infraestructura pueden experimentar reestructuraciones drásticas debido a que la mayor parte de sus obligaciones pasan a ser desempeñadas por el proveedor del servicio.
- **Confianza:** esta recae sobre el proveedor de la nube aunque existe la posibilidad de que el servicio se “caiga”, sin que el

departamento de sistemas de la compañía pueda hacer algo más que esperar; los niveles de eficiencia de los proveedores de nube no son menores del 99%.

**Tabla 2: Administración de componentes en los diferentes servicios**

| Ambiente local | IaaS | PaaS | SaaS |
|---|---|---|---|
| Aplicaciones | Aplicaciones | Aplicaciones | Aplicaciones |
| Datos | Datos | Datos | Datos |
| Runtime | Runtime | Runtime | Runtime |
| Middleware | Middleware | Middleware | Middleware |
| Sistema Operativo | Sistema Operativo | Sistema Operativo | Sistema Operativo |
| Virtualización | Virtualización | Virtualización | Virtualización |
| Servidores | Servidores | Servidores | Servidores |
| Almacenamiento | Almacenamiento | Almacenamiento | Almacenamiento |
| Redes | Redes | Redes | Redes |

**Administrado por la Compañía** **Administrado por el Proveedor**

## 3.2 Estadísticas de empresas proveedoras de software ERP en la nube que poseen la certificación ISO 27018:2014

En el 2016, los 10 principales proveedores de software ERP representaron casi el 29% del mercado global de aplicaciones ERP; el cual creció 1.4%

con respecto al año anterior a ese acercándose a casi $82.2 mil millones en ingresos por licencia, mantenimiento y suscripción.

SAP lideró con casi el 7% de participación de mercado, cerca de $5.6 mil millones en ingresos de productos ERP seguido de FIS Global y Oracle. A continuación el gráfico nos indica los primeros 10 proveedores de Software:

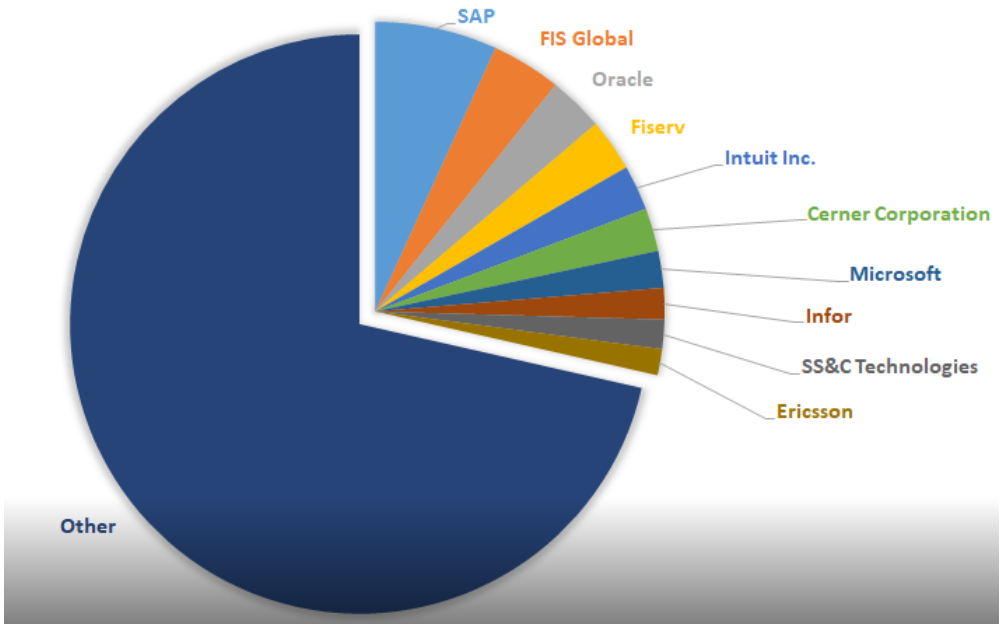



**Figura 3.7: Top 10 de Proveedores de ERP en 2016**

Entre los datos obtenidos con la investigación, el reporte brinda las siguientes estadísticas:

- La mayoría de las organizaciones no tienen experiencia interna para lograr el éxito de ERP y necesitan especialistas del exterior para ayudarlos a obtener los máximos beneficios y el ROI potencial.

- El 35% informó sobre los costos de implementación que fueron entre 1 – 3% de los ingresos anuales de su organización, mientras que el 20% informó sobre los costos de implementación que fueron entre 3 – 5% de sus ingresos anuales; en las organizaciones restantes los costos de implementación fueron superiores al 5%.
- En promedio, el proyecto ERP representa el 6.5% de los ingresos anuales de las organizaciones, lo que representa un aumento respecto de la cifra del 5.9% en 2015.
- En los resultados de Implementación del ERP, el 57% informó éxito, el 36% no lo sabía y el 7% informó fracaso.
- Los resultados de implementación de ERP a menudo estaban nublados por la confusión y la neutralidad que indican que las organizaciones no dedicaron suficiente tiempo a seleccionar el software, justificar el caso de negocios, medir la realización de beneficios o auditar la implementación posterior.
- El 56% de las organizaciones seleccionaron el software local entre sus opciones de implementación, mientras que el 27% eligió la nube y el 17% optó por SaaS.
- Se ha producido un salto significativo en el uso del ERP en la nube, del 11% en 2015 al 27% en 2016, que fue en gran medida provocado por más proveedores que ofrecen plataformas en la nube.

### 3.2.1 Principales Proveedores de SaaS ERP que dominan el mercado actual

Las soluciones ERP de Software como Servicio (SaaS) se está acelerando como un modelo de entrega convencional para ayudar a las empresas a obtener flexibilidad y así aprovechar las tecnologías de nube modernas; el panorama del mercado muestra a los proveedores de ERP tradicionales que están llevando sus ofertas hacia la nube para no perder terreno frente a los proveedores de soluciones de ERP de nube pura. En la tabla del Anexo B podemos ver información sobre los principales proveedores que poseen la mayor parte del mercado de SaaS ERP:

## 3.3 Levantamiento de información del ERP en la nube ofrecido por la empresa Ecuatoriana desarrolladora del Software

### 3.3.1 Inventario y Clasificación de Activos

Se han identificado los activos de información considerados Críticos para la Continuidad de los servicios que brinda la Empresa Desarrolladora del Software. Según el tipo de activo están clasificados en:

- **Software:** trata sobre los programas, aplicativos y los desarrollos que permiten el normal funcionamiento de la empresa.
- **Hardware:** son los medios físicos que se utilizan para almacenar y trabajar sobre los aplicativos y desarrollos.
- **Recurso Humano:** es el personal humano que está a cargo de las actividades en la empresa desarrolladora del software.
- **Comunicaciones:** medio que se usa para acceder a los sistemas para su monitoreo, control y actualización.
- **Información:** los datos que permiten el correcto funcionamiento de la aplicación y de la empresa.
- **Infraestructura:** equipos utilizados para procesar la información de los aplicativos, desarrollos, etc.

**Tabla 3: Inventario de activos**

| **Inventario de Activos** | |
|---|---|
| **Tipo de Activo** | **Cantidad de Activos** |
| Hardware | 5 |
| Información | 7 |
| Instalaciones | 1 |
| Recurso Humano | 2 |

| Inventario de Activos | |
|---|---|
| **Tipo de Activo** | **Cantidad de Activos** |
| Servicio | 3 |
| Software | 4 |

### 3.3.2 Valoración de activos

Se realiza la valoración de activos en Confidencialidad, Integridad, Disponibilidad e Importancia:

**Tabla 4: Valoración del Activo**

| Valoración del Activo | | | | |
|---|---|---|---|---|
| **Valor** | **Confidencialidad** | **Disponibilidad** | **Integridad** | **Importancia** |
| 1 | No Aplica | No Aplica | No Aplica | No Aplica |
| 2 | Pública | Muy Bajo | Muy Bajo | Muy Bajo |
| 3 | Uso Interno | Bajo | Bajo | Bajo |
| 4 | Uso Restringido | Medio | Medio | Medio |
| 5 | Confidencial | Alto | Alto | Alto |
| 6 | Secreto | Crítico | Crítico | Crítico |

**Tabla 5: Importancia del Activo**

| **Importancia del Activo** | | |
|---|---|---|
| **Estimación Cuantitativa** | **Estimación Cualitativa** | **Descripción** |
| 1 | No Aplica | Sin nivel de importancia para el activo. |
| 2 | Muy Bajo | El activo no afectará el proceso. |
| 3 | Bajo | La afectación del activo sería menor en cuanto a la operación. |
| 4 | Medio | Se puede afectar de forma parcial la operación. |
| 5 | Alto | La operación puede verse afectada seriamente. |
| 6 | Crítico | La operación se ve afectada seriamente incluida su credibilidad y genera sanciones a la organización. |

# CAPÍTULO 4

## Análisis y Diseño de la Solución ERP en la Nube

### 4.1 Análisis de Riesgos en Computación en la Nube

En el presente capítulo vamos a presentar los diferentes riesgos de la computación en la nube, lo primero que debemos hacer es entender la definición de Riesgo. La norma ISO 31000 define el riesgo como el efecto de la incertidumbre en los objetivos establecidos por una organización, la incertidumbre es el efecto de fuerzas externas e internas de las que la organización no tiene el control total.

### 4.1.1 Riesgos para la Seguridad y Privacidad de los datos

A medida que los datos cruzan los límites tradicionales de la empresa, dejan de estar sujetos a las medidas de seguridad física de la empresa, como lo son el control de acceso físico a las ubicaciones de la empresa o las medidas técnicas de seguridad que protegen los sistemas de información [9].

**Confidencialidad de los datos:** La nube presenta desafíos adicionales a la confidencialidad de los datos. La apertura de la nube pública significa que hay múltiples usuarios para los mismos recursos, lo que aumenta el riesgo de acceso no autorizado. Debido al gran volumen de datos y transacciones, también las medidas de seguridad deben ser capaces de manejar mucha más información que una infraestructura tradicional.

**Integridad de los datos:** Se puede lograr asegurando que todos los procesos que modifican los datos tengan en cuenta la atomicidad, consistencia, aislamiento y durabilidad de los datos. Para garantizar esto, es imperativo que solo aquellos que estén autorizados puedan acceder a los datos y modificarlos, es igualmente importante diferenciar en qué formas determinados

usuarios pueden modificar los datos, algunos usuarios tienen más privilegios que otros.

**Disponibilidad de datos:** Como tercer componente de la seguridad de los datos tenemos la Disponibilidad de los mismos. Poder acceder a los datos críticos de la empresa en todo momento es una de las mayores preocupaciones de las empresas cuando consideran trasladar sus datos y aplicaciones a la nube. Se espera que la disponibilidad de la nube coincida o incluso exceda la disponibilidad de la infraestructura interna equivalente. La alta disponibilidad es posible gracias a un análisis exhaustivo de la demanda real de servicios en la nube.

**Ubicación de datos:** La ubicación de los datos es un aspecto de la seguridad especialmente relevante cuando está en juego información confidencial y de identificación personal (PII), a que dichos datos están sujetos a estrictas regulaciones con respecto al almacenamiento y eliminación.

**Privacidad de datos:** La privacidad es una parte elemental de la seguridad de la computación en la nube, al tratarse del derecho de un individuo u organización a decidir cómo, cuándo y cuánta

información sobre ellos está disponible. El cifrado es una herramienta muy efectiva para proteger la privacidad de los datos, pero esta efectividad afecta negativamente la facilidad de uso de los datos, ya que realizar las operaciones informáticas, especialmente buscar e indexar los datos, es difícil cuando los datos están cifrados [10].

### 4.1.2 Riesgos Tecnológicos de Seguridad

No existe un concepto aislado o claramente definible de tecnología en la nube, debido a que la nube consiste en una combinación de tecnologías diferentes; antiguas y nuevas, que en conjunto forman la nube.

Los riesgos relacionados con las tecnologías más importantes que permiten la computación en la nube son: la virtualización, las tecnologías web y las tecnologías de administración de identidades y acceso [11].

**Riesgos de Virtualización:** La virtualización es la columna vertebral tecnológica de la computación en la nube, lo que hace posible el aprovisionamiento dinámico de recursos. La virtualización

es posible gracias a un hipervisor, también conocido como monitor de máquina virtual; como el hipervisor incluye significativamente menos código que un sistema operativo completo, en teoría, su seguridad es más fácil de verificar y mantener que la de un sistema operativo. Sin embargo por el rápido desarrollo en la nube ha hecho que los monitores de máquina virtual sean más complicadas, lo que complica la administración de la seguridad; todas las operaciones de procesamiento realizadas en la nube se enrutan a través del hipervisor, convirtiéndolo en una fuente de riesgo muy importante.

**Problemas de seguridad presentes en la tecnología de virtualización:**

- Salto de máquinas virtuales (VM Hopping).
- Movilidad de máquinas virtuales (VM Mobility).
- Diversidad de máquinas virtuales (VM Diversity).
- Denegación de servicio de máquinas virtuales (VM Denial of Service).

**Riesgos en las tecnologías web:** siempre se accede a los servicios a través de una conexión de red utilizando un navegador web, las tecnologías web son una parte esencial de la nube e incluyen muchas vulnerabilidades que presentan riesgos para la computación en la nube [12].

La lista de riesgos en tecnologías web del 2017 fueron las siguientes:

- Inyección (Injection).
- Autenticación Rota (“Broken Authentication”).
- Exposición de datos sensibles (“Sensitive Data Exposure”).
- Entidades Externas XML (“XML External Entities – XXE”).
- Control de Acceso Roto (“Broken Access Control”).
- Mala Configuración de Seguridad (“Security Misconfiguration”).
- Secuencias de comandos entre sitios (“Cross-Site Scripting – XSS”).
- Deserialización insegura (“Insecure Deserialization”).
- Uso de componentes con vulnerabilidades conocidas (“Using Components with Known Vulnerabilities”).
- Insuficiente Registro y Monitoreo (“Insufficient Logging&Monitoring”).

**Riesgos en la gestión de identidad y acceso:** la gestión de identidad y acceso o IAM es un concepto que permite la identificación de usuarios y la gestión de su acceso a los recursos; además de proporcionar acceso, la otra parte igualmente de la IAM es evitar el acceso no autorizado.

La Gestión de Identidad y Acceso también proporciona las capacidades de autenticación, autorización y auditoria. La autenticación es el proceso de verificación de la identidad del usuario, mientras que la autorización verifica los privilegios del usuario; la auditoría es el proceso de monitoreo de los procesos de autenticación y autorización, tiene un papel crítico en la detección de accesos no autorizados y posibles violaciones.

### 4.1.3 Identificación de Amenazas

Realizando la identificación de amenazas que pueden afectar a nuestros activos, se realizó un listado de acuerdo al catálogo de amenazas de Magerit; el cual se detalla en el Anexo “C”.

Se utilizará la metodología Magerit[1], la cual permite la identificación, análisis y valoración de riesgos. Con esta metodología, elaborada por el CSAE[2] se procederá a identificar y analizar las amenazas y sus posibles consecuencias o nivel de impacto.

[1] : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

[2] : Consejo Superior de Administración Electrónica

### 4.1.4 Matriz de Análisis de Riesgos

En la identificación de las Amenazas se pudieron detectar 25 de las cuales se ha identificado 11 Riesgos entre Inherentes y Residuales.

Para realizar un análisis y diagnóstico de los riesgos más detallado debemos entender cuál va a ser el criterio de valoración con respecto a la Probabilidad de Ocurrencia; los cuales se detallan en la siguiente Tabla:

**Tabla 6: Probabilidad de Ocurrencia**

| **Probabilidad de Ocurrencia** | | |
|---|---|---|
| **Valor Cuantitativo** | **Valor Cualitativo** | **Descripción** |
| 5 | Frecuente | El evento ocurre en un corto periodo de tiempo, frecuentemente. Más de 1 vez al año. |
| 4 | Probable | Muy probable de que ocurra en la mayoría de las circunstancias. Al menos 1 vez al año. |
| 3 | Ocasional | Es probable que ocurra en algún momento. Al menos 1 vez en los 2 últimos años. |
| 2 | Improbable | No es probable que ocurra el evento pero si es posible. Al menos 1 vez en los últimos 5 años. |
| 1 | Raro | Es improbable que ocurra el evento, sólo en circunstancias excepcionales. No ha ocurrido en los últimos 5 años. |

**Tabla 7: Impacto o efecto del Riesgo**

| Impacto o Efecto del Riesgo | | |
|---|---|---|
| **Valor Cuantitativo** | **Valor Cualitativo** | **Descripción** |
| 5 | Catastrófico | Cuando el evento se presenta con consecuencias negativas para la entidad. |
| 4 | Mayor | El evento al presentarse tiene alto impacto o efecto para la entidad. |
| 3 | Moderado | El evento presenta medianas consecuencias para la entidad. |
| 2 | Menor | El evento tendría un bajo impacto o efecto para la entidad. |
| 1 | Insignificante | De presentarse el evento tendría un impacto o efecto mínimo sobre la entidad. |

**Tabla 8: Probabilidad e Impacto del Riesgo**

| **Probabilidad** | **Impacto - Consecuencia** | | | | |
|---|---|---|---|---|---|
| | **Insignificante** | **Menor** | **Moderado** | **Mayor** | **Catastrófico** |
| Raro | Bajo | Bajo | Moderado | Alto | Extremo |
| Improbable | Bajo | Bajo | Moderado | Alto | Extremo |
| Ocasional | Bajo | Moderado | Alto | Extremo | Extremo |
| Probable | Moderado | Alto | Alto | Extremo | Extremo |
| Frecuente | Alto | Alto | Extremo | Extremo | Extremo |

### 4.1.5 Matriz de Evaluación de Riesgos

En base al análisis que se realizó de las amenazas y vulnerabilidades se obtuvo como resultado la siguiente Matriz de Riesgos:

**Tabla 9: Matriz de Riesgos (Inventario)**

| Impacto | Cantidad | Tipo de Riesgo | Tipo de Amenazas | Tipo de Activo |
|---|---|---|---|---|
| **Extremo** | 10 | 9 Residuales<br>1 Inherente | 4 Accidental<br>4 Deliberado<br>2 Entorno | 5 Hardware<br>4 Software<br>1 Instalaciones |
| **Alto** | 12 | 10 Residuales<br>2 Inherente | 5 Accidental<br>7 Deliberado | 4 Hardware<br>3 Software<br>1 Redes<br>2 Información<br>1 Recurso Humano<br>1 Servicio |
| **Moderado** | 5 | 3 Residuales<br>2 Inherentes | 2 Accidental<br>3 Deliberado | 2 Software<br>1 Redes<br>1 Recurso Humano<br>1 Información |
| **Bajo** | 2 | 2 Residuales | 1 Accidental<br>1 Deliberado | 1 Hardware<br>1 Software |

## 4.2 Requerimientos de Diseño de la solución enfocándonos en los controles para el Control de Acceso

Con la Matriz de Riesgos elaborada en la cual se ha logrado la identificación y valoración de los riesgos se procederá a la evaluación de los Controles de la Norma ISO/IEC 27001:2013, los cuales deberán ser implementados para el tratamiento de riesgos.

La selección de controles depende de las decisiones organizativas basadas en los criterios de aceptación del riesgo, las opciones de tratamiento del riesgo y el enfoque general de gestión del riesgo aplicado a la organización y a través de acuerdos contractuales, a sus clientes y proveedores [13].

Las acciones serán: Mitigar, Aceptar, Transferir o Eliminar, de las que se detalla su definición en la siguiente tabla:

**Tabla 10: Matriz de Riesgos**

| Acción de Tratamiento | Descripción |
|---|---|
| Mitigar | Consiste en la reducción o eliminación de los riesgos existentes. |
| Aceptar | Aceptamos un riesgo cuando la frecuencia es baja o el impacto es leve. |

| Acción de Tratamiento | Descripción |
|---|---|
| Transferir | Se transfiere el riesgo para compartir la responsabilidad con terceros. |
| Eliminar | Eliminación del riesgo del ambiente laboral para mantenerlos alejados de la empresa. |

Para gestionar adecuadamente los riesgos de la seguridad de la información identificados, se tomaran medidas para la reducción o eliminación de los riesgos:

- Implementación de un Proveedor de Servicios Cloud de Contingencia.
- Capacitación especializada constante al personal.
- Actualización del Plan de Continuidad del Negocio.
- Actualización de los equipos activos de Red.
- Modernización de los equipos de Seguridad de Información.
- Adquirir Generador.
- Asignación de responsabilidades de seguridad de la información a personal.

En el Anexo F se detalla la implementación de las medidas adoptadas.

## 4.3 Diseño de la solución basada en la norma ISO 27018:2014 para un servicio SaaS

En el esquema de Diseño actual se basa en Software como Servicio (SaaS), las aplicaciones son entregadas a través de internet en forma de servicio evitando la instalación de Software [14].

La solución posee las siguientes características de Diseño:

- **Posee Arquitectura Multiarrendatario:** varios usuarios y aplicaciones comparten un código fuente común el cual se mantiene centralmente en una ubicación.
- **Personalización:** Dado que el código fuente se mantiene en un solo lugar, es más fácil personalizar la aplicación en función de las necesidades comerciales del cliente.
- **Accesibilidad:** Proporciona un mejor acceso a los datos a través de Internet. Esto hace que sea más fácil administrar privilegios o monitorear el uso de datos. También asegura que la misma información esté disponible para todos los usuarios en cualquier momento.

## 4.4 Análisis de Costos de la solución

Al tratarse de una solución cuya implementación se realizó completamente en la nube los costos son en base a las tarifas que mantienen los proveedores de Computación en la nube. A continuación se presentan los

costos mensuales por el alquiler de la infraestructura para la solución SaaS, se evaluaron dos proveedores los cuales son Microsoft Azure y 1and1.

Las propuestas deben contener los siguientes elementos como principales:

- Procesador de 4 núcleos con 16GB de RAM.
- Almacenamiento de 1000GB con respaldo de la información.
- Sistema Operativo a utilizarse es Linux Centos.

Microsoft Azure Estimate

Su presupuesto

| Service type | Custom name | Region | Description | Estimated Cost |
|---|---|---|---|---|
| Virtual Machines | | East US | 1 D4 v3 (4 vCPU; 16 GB de RAM) x 730 Hours; Linux – CentOS; Pago por uso; 0 discos de sistema operativo administrados: S15, 100.000 unidades de transacción | $190,16 |
| Storage | | East US | Redundancia Table Storage, Estándar y LRS, Capacidad: 1.000 GB, Transacciones de Storage: 100000 | $106,00 |
| Virtual Network | | | 1000 GB de transferencia de datos de la región Este de EE. UU. a la región Este de EE. UU. | $20,00 |
| Support | | | Support | $100,00 |
| | | | Licensing Program | Microsoft Online Services Program (MOSP) |
| | | | Monthly Total | $416,16 |
| | | | Annual Total | $4.993,92 |

**Figura 4.8: Costo por uso de la nube de Azure para la solución**

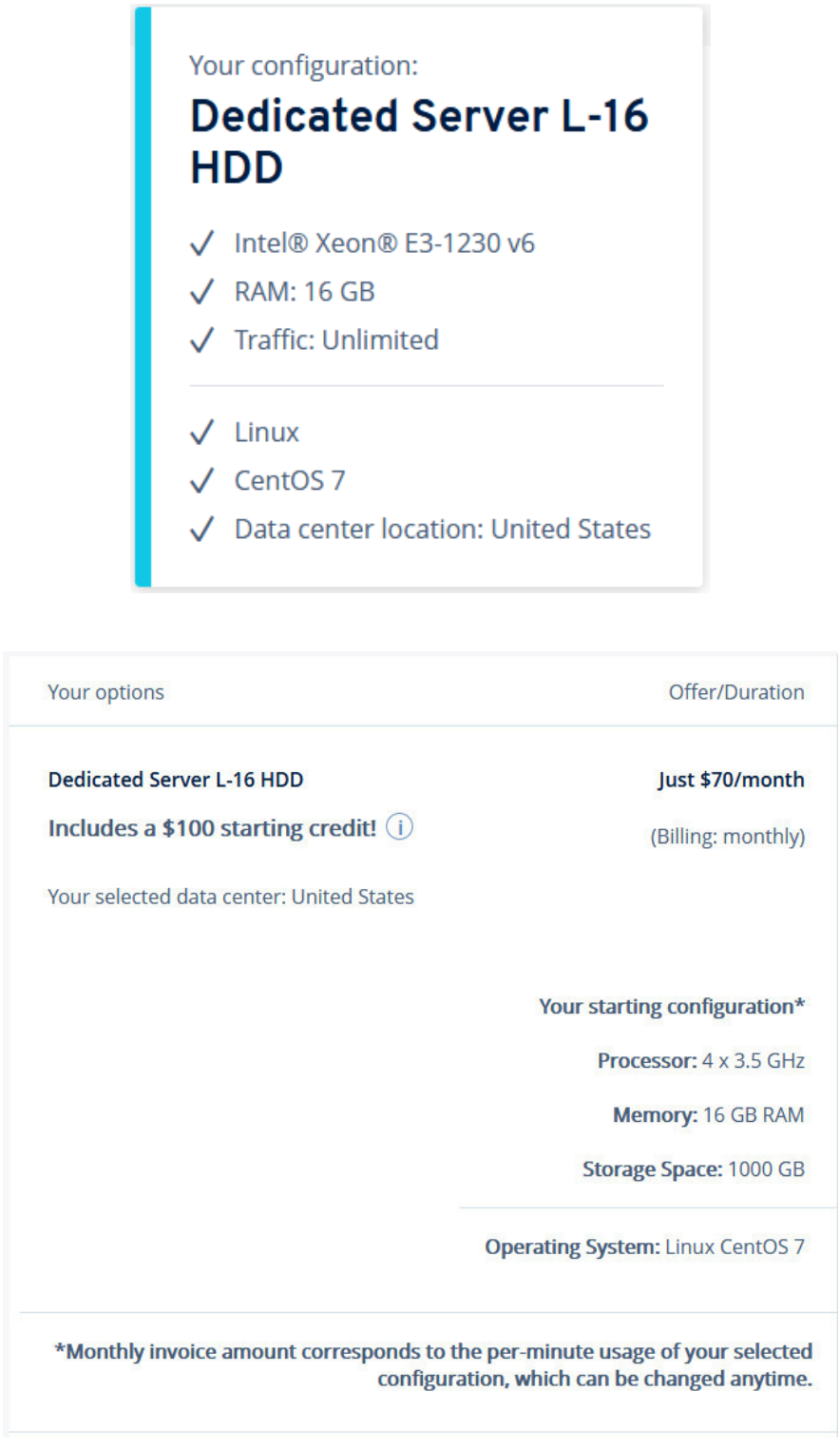



**Figura 4.9: Costo por uso de la nube de 1and1 para la solución**

De las opciones mostradas la opción elegida es la de 1and1 la cual tiene un valor mensual inferior al de Azure y proporciona confianza y rapidez en cuanto a su servicio.

# CAPÍTULO 5

## Implementación de los Controles de la Norma ISO 27018:2014

### 5.1 Definición de los Controles basados en la información obtenida en el Levantamiento de Información y Análisis de la Solución

Los controles a definirse en el presente proyecto son aquellos necesarios para el tratamiento de los riesgos actuales de la Empresa Desarrolladora de Software; los mismos que se encuentran detallados en el Anexo F.

### 5.2 Implementación de los controles que brinden un adecuado Control de Acceso a la solución

En la actualidad, los buenos controles de seguridad de la información no consisten en obligarse a tomar medidas para enfrentar las presiones externas, sino a reconocer el valor positivo de la buena práctica de los controles de seguridad de la información que se está incorporando en la organización.

## 5.3 Declaración de Aplicabilidad de los controles para la solución ERP

En el Anexo G se incluye la Declaración de Aplicabilidad para el tratamiento de los riesgos encontrados y que faciliten el correcto proceso de Continuidad de los Servicios.

# CAPÍTULO 6

## Análisis de los resultados

### 6.1 Confiabilidad en el cumplimiento de obligaciones legales y otras por parte de la solución con la implementación

Hoy en día es muy evidente que la Seguridad de la Información juegue un papel importante en las organizaciones, debido a que la llegada de nuevas tecnologías expone a amenazas a la información.

Los mecanismos que se implementan para proteger los activos deben de garantizar todas las dimensiones de la seguridad de la información como

lo son: no repudio, integridad, disponibilidad, autenticidad, confidencialidad y conservación de la información.

- **Mecanismos para garantizar la disponibilidad de los recursos de la red y sus servicios:** consisten en la modernización de la infraestructura tecnológica así como de seguridad de la información.
- **Mecanismos para garantizar la integridad de la información, servicios, sistemas y demás recursos de red:** los datos deben conservarse tal cual fueron almacenados por el usuario autorizado, para lograr esto deben utilizarse certificados de seguridad o firmas electrónicas.
- **Mecanismos para garantizar la autenticidad de la información:** mediante la modernización de la infraestructura y la seguridad de la información estas tendrán las capacidades de verificar la identidad de los usuarios y los sistemas.
- **Mecanismos para garantizar la confidencialidad:** la codificación es un componente clave que asegura que solo tengan acceso a la información el personal clave, para esto se incluye en los controles la implementación de mecanismos de cifrado.
- **Garantizar el No Repudio:** se establecen mecanismos para el control y protección y sólo los propietarios de la información sean capaces de controlarla en todo momento evitando perder el control en favor de agentes maliciosos.

## 6.2 Facilidad para la creación de los controles de los servicios del ERP en la Nube

Luego de la evaluación de los riesgos y amenazas existentes, se han establecido controles en diferentes áreas; cuya implementación estará guiada por la Dirección de la organización así como por el resto del personal.

Existe una gran apertura para la implementación de los controles, ya que se reconoce su importancia para la operación continua de los servicios; en base a esto se realizó un Plan de Tratamiento de Riesgos en el Anexo E en el cual se establecen fechas para la implementación de los proyectos que ayudaran a conseguir los objetivos trazados.

## 6.3 Confianza en los servicios brindados en lo referente a la protección de sus datos

La confianza debe ser originada por parte de la empresa desarrolladora del software y que ofrece el servicio; esto debido a que es el principal factor de riesgo para el cliente. Ya que si existe algún caso de fuga de información causada por la empresa desarrolladora del software esto afectará las operaciones del cliente y la reputación del proveedor.

En la actualidad la empresa desarrolladora del software no ha tenido incidentes en los que se vean afectadas sus operaciones, logrando así que día a día su plataforma sea utilizada por más y más clientes quienes ven como factor diferenciador la confianza qué ésta brinda en sus operaciones.

# CONCLUSIONES Y RECOMENDACIONES

## CONCLUSIONES

1. El análisis del proceso de continuidad de las operaciones de la empresa desarrolladora del software permitió conocer que ciertos servicios críticos se podrían ver afectados en cuanto a su disponibilidad.
2. El levantamiento de información permitió conocer los activos con los que cuentan y los cuales deben protegerse en cuanto a la valorización de su importancia para las operaciones así como los que necesitan de un plan de actualización.
3. Con la elaboración de la matriz de riesgos se pudo conocer la situación real de la empresa en cuanto a la seguridad de sus activos y cómo puede esto afectar a la productividad de la organización.
4. Con el Plan de Tratamiento de Riesgos se visualiza implementar los cambios necesarios para mejorar la seguridad de la infraestructura y

obtener un Plan de Continuidad de las operaciones que mejoren la imagen de la organización frente a los clientes.

## RECOMENDACIONES

1. Ejecutar de forma periódica la actualización de los activos con la finalidad de mantenerlos valorizados para un correcto funcionamiento de las operaciones.
2. Realizar la revisión y actualización de su Plan de Continuidad del Negocio de forma periódica y así estar siempre preparados ante eventuales incidentes.
3. Socializar siempre los procedimientos que involucren a su personal interno así como con sus clientes y proveedores, esto mantendrá siempre una imagen de confianza.

# BIBLIOGRAFÍA


[1] 27001 Academy, http://www.iso27001standard.com/es, fecha de consulta Enero 2019

[2] Implantación de un SGSI en la empresa, https://www.incibe.es, fecha de consulta Diciembre 2018

[3] Melaños Salazar Carla, Análisis de los riesgos técnicos y legales de la seguridad en Cloud Computing, http://www.dit.upm.es/~posgrado/doc/TFM/TFMs2012-2013/TFM_Carla_Melanos_2013.pdf, fecha de consulta Enero 2019

[4] Ecuador, Acuerdo Ministerial No. 166, "Esquema Gubernamental de Seguridad de la Información ESGI", Suplemento 88 Fecha 25 de septiembre de 2013, Fecha modificado 15 de Junio de 2016.

[5] BSI Standards Publication, Information technology - Security techniques - Code of practice for information security controls, http://www.smartassessor.com/Uploaded/1/Documents/ISO-2017-standard.pdf, fecha de consulta Noviembre 2018

[6] ISO 27001 en Wikipedia, http://es.wikipedia.org/wiki/ISO/IEC_27001.

[7] España, Ministerio de Hacienda y Administraciones Públicas, Secretaría General Técnica, MAGERIT – versión 3.0 Metodología y análisis de gestión de

riesgos de los sistemas de seguridad de información. Libro I “Método”. Fecha Octubre de 2012.

[8] España, Ministerio de Hacienda y Administraciones Públicas, Secretaría General Técnica, MAGERIT – versión 3.0 Metodología y análisis de gestión de riesgos de los sistemas de seguridad de información. Libro II “Catalogo de Elementos”, Fecha Octubre de 2012.

[9] Aenor, Privacidad elevada a la nube, http://www.normas-iso.com/2015/iso-iec-27018-2014-requisitos-para-la-proteccion-de-la-informacion-de-identificacion-personal, fecha de consulta Diciembre 2018

[10] España, Ministerio de Hacienda y Administraciones Públicas, Secretaría General Técnica, MAGERIT – versión 3.0 Metodología y análisis de gestión de riesgos de los sistemas de seguridad de información. Libro III “Guía de Técnicas”. Fecha Octubre de 2012.

[11] INEN, https://inen.isolutions.iso.org/obp/ui/#iso:std:iso-iec:27018:ed-1:v1:en, fecha de consulta Enero 2019

[12] OWASP, https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf, fecha de consulta Febrero 2019

[13] Kaushik Pal, 11 Essential Steps for Implementing SaaS, https://www.techopedia.com/2/31093/trends/virtualization/11-essential-steps-for-implementing-saas, fecha de consulta Febrero 2019

[14] Strickland Jonathan, How Cloud Computing Works, https://computer.howstuffworks.com/cloud-computing/cloud-computing1.htm, fecha de consulta Noviembre 2018

[15] El Portal de ISO 27001 en Español, http://www.iso27000.es, fecha de consulta Noviembre 2018

# GLOSARIO

**API (Application Programming Interface) - Interfaz de programación de aplicaciones:** permite que aplicaciones de terceros puedan solicitar datos, es el mecanismo más utilizado de comunicación entre aplicaciones.

**Backup:** copia de seguridad realizada a aplicaciones o datos con la finalidad de poder recuperar la información en caso de desastre.

**Cloud Computing (Computación en la Nube):** concepto tecnológico que se basa en la capacidad de proceso y almacenaje de datos que no están en la PC a los cuales se acceden a través de Internet.

**IaaS (Infraestructure as a Service) – Infraestructura como Servicio:** es un servicio basado en virtualización en el cual se paga por consumo de los recursos, sean este espacio en disco duro, tiempo de CPU o transferencia de Datos.

**Nube Pública:** es el modelo en el cual el prestador del servicio pone a disposición de cualquier usuario en Internet su Infraestructura.

**Nube Privada:** es el modelo en el cual los servicios se ofrecen en la infraestructura del cliente.

**PaaS (Platform as a Service) – Plataforma como Servicio:** este modelo permite desarrollar e implantar aplicaciones desde Internet.

**SaaS (Software as a Service) – Software como Servicio:** se trata de aplicaciones ofrecidas por su creador a través de Internet para la utilización de varios clientes.

# ANEXOS

## ANEXO A - NORMAS ISO 27000

Los estándares publicados de la serie ISO 27000 [15] son:

- **ISO/IEC 27000:2016:** su cuarta y más reciente edición fue lanzada en Febrero del 2016 y recoge la visión general de las normas de la serie 27000 así como el alcance y propósito de cada una de ellas.
- **ISO/IEC 27003:** desarrollada principalmente para centrarse en los aspectos críticos necesarios para el éxito en el diseño e implementación de un SGSI de acuerdo a la norma ISO/IEC 27001; la edición más reciente es la del 12 de abril del 2017.
- **ISO/IEC 27004:** su última edición fue revisada en Diciembre del 2016 y corresponde a una guía para seguir para el desarrollo y utilización de métricas y técnicas de medidas para conocer la eficacia de un SGSI y los controles o grupos de controles implementados según ISO/IEC 27001.
- **ISO/IEC 27005:** sirve de apoyo para los conceptos generales de la norma ISO/IEC 27001:2005 al proporcionar directrices para la administración del riesgo en la seguridad de la información; su edición

más actual es la segunda el 1 de junio del 2011 y actualmente está en un proceso de revisión.

- **ISO/IEC 27006:** esta norma fue revisada y actualizada el 30 de Septiembre del 2015, la misma sirve para validar los requisitos para la acreditación de las entidades de auditoria y certificación de sistemas de gestión de seguridad de la información aún sin ser una norma de acreditación por sí misma.
- **ISO/IEC 27007:** es un complemento a la ISO 19011 y sirve como guía de un SGSI, su revisión más reciente fue el 9 de Octubre del 2017.
- **ISO/IEC TR 27008:** se encuentra actualmente en proceso de revisión y sirve de guía para la auditoría de los controles seleccionados en el marco de implantación de un SGSI.
- **ISO/IEC 27009:** se trata de una publicación muy reciente, en Junio del 2016 y contempla los requisitos para usar la ISO/IEC 27001 en sectores específicos, como campo, área de aplicación o sector industrial.
- **ISO/IEC 27010:** nos brinda una guía para administrar la seguridad de la información cuando se participa entre entidades o sectores, se puede aplicar tanto a entes públicos como privados y es aplicable a todas las formas de intercambio y difusión de información sensible. Su última revisión fue en Noviembre del 2015.
- **ISO/IEC 27011:** elaborada para servir de guía para la implementación y gestión de la seguridad de la información en el sector de

telecomunicaciones. Su última revisión fue en Diciembre del 2016 y está basada en ISO/IEC 27002.

- **ISO/IEC 27013:** es un complemento como guía de implementación integrada de ISO/IEC 27001:2005 y de la ISO/IEC 20000-1, fue actualizada en Noviembre del 2015.
- **ISO/IEC 27014:** sirve de guía de gobierno corporativo de la seguridad de la información y fue publicada en Abril del 2013.
- **ISO/IEC TR 27015:** fue publicada en Noviembre del 2012 siendo una guía de SGSI que está orientada al sector financiero y de seguros, actúa como un complemento a ISO/IEC 27002:2005.
- **ISO/IEC TR 27016:** su publicación se dio en Febrero de 2014 y sirve de guía de la valoración de los aspectos financieros de la seguridad de la información.
- **ISO/IEC 27017:** se la elaboró pensando en que sea una guía de seguridad para Computación en la Nube en Diciembre del 2015 y está alineada con ISO/IEC 27002, además que también contempla ciertos controles adicionales específicos para entornos de nube.
- **ISO/IEC TR 27019:** hace referencia a la ISO/IEC 27002:2005 en cuanto al proceso de sistemas de control relacionados con el sector de la industria de la energía, fue publicada en Julio del 2013.

- **ISO/IEC 27021:** se está desarrollando enfocada en los requisitos de las competencias requeridas por los profesionales que están dedicados a los sistemas de gestión para la seguridad de la información.
- **ISO/IEC TR 27023:** fue publicada en Julio del 2015 y es vista como una guía de correspondencias entre las normas ISO/IEC 27001 e ISO/IEC27002 en las versiones del 2013 apoyando a la transición de las versiones publicadas en 2005.
- **ISO/IEC 27031:** basándose en el estándar BS 25777 sirve de guía de apoyo para la adecuación de las TIC de una organización para la continuidad del negocio.
- **ISO/IEC 27032:** sirve de guía para la mejora de la seguridad cibernética cubriendo las prácticas de seguridad básica para los interesados en el ciberespacio, fue publicada en Julio de 2012.
- **ISO/IEC 27033:** está dedicada a la seguridad en redes y consiste de 6 partes:
    - Conceptos generales.
    - Directrices de diseño e implementación de seguridad en redes.
    - Escenarios de referencia de redes.
    - Aseguramiento de las comunicaciones entre redes mediante gateways (Puertas de enlace) de seguridad.
    - Aseguramiento de comunicaciones mediante VPNs (Redes Privadas Virtuales).

- Seguridad en el acceso de redes IP Wireless.

Estas partes han sido publicadas en diferentes años a partir del 2009 hasta el 2016.

- **ISO/IEC 27034:** guía sobre Seguridad en aplicaciones informáticas, consiste en 7 partes:
  - Conceptos generales.
  - Marco normativo de la organización.
  - Proceso de gestión de seguridad en aplicaciones (en desarrollo).
  - Validación de la seguridad en aplicaciones.
  - Estructura de datos, protocolos y controles de seguridad de aplicaciones.
  - Guía de seguridad para aplicaciones de uso específico.
  - Marco predictivo de la seguridad (en desarrollo).
- **ISO/IEC 27035:** es una orientación sobre la gestión de incidentes de seguridad en la información y está compuesta de 3 partes:
  - Principios en la gestión de incidentes.
  - Guías para la elaboración de un plan de respuesta a incidentes.
  - Guía de operaciones en la respuesta a incidentes.
- **ISO/IEC 27036:** se enfoca en la seguridad en las relaciones con proveedores y consta de cuatro partes:
  - Visión general y conceptos.

  - Requisitos comunes.
  - Seguridad en la cadena de suministro TIC.
  - Guía de seguridad para entornos de servicios Cloud.
- **ISO/IEC 27037:** nos brinda directrices para la identificación, recopilación, consolidación y preservación de evidencias digitales localizadas en los diferentes dispositivos electrónicos; fue publicada en Octubre 2012.
- **ISO/IEC 27038:** fue publicada en Marzo del 2014 y sirve como guía de especificación para seguridad en la redacción digital.
- **ISO/IEC 27039:** está orientada en la selección, despliegue y parte operativa de sistemas de prevención de intrusos (IDS/IPS), fue publicada en Febrero de 2015.
- **ISO/IEC 27040:** nos sirve de guía en la seguridad de medios de almacenamiento y fue publicada en Enero de 2015.
- **ISO/IEC 27041:** fue publicada en Junio de 2015 y garantiza la idoneidad y adecuación de los métodos de investigación.
- **ISO/IEC 27042:** es una guía que maneja directrices para análisis e interpretación de evidencias digitales; fue publicada en Junio 2015.
- **ISO/IEC 27043:** es una guía que presenta el desarrollo de principios y procesos de investigación para la recopilación de evidencias digitales, fue publicada en Marzo 2015.

- **ISO/IEC 27050:** fue desarrollada como guía para el manejo de la información almacenada en dispositivos electrónicos para su identificación, preservación, recolección, procesamiento, revisión, análisis y producción, consta de tres partes:
  - Conceptos generales.
  - Guía para el gobierno y gestión (en desarrollo).
  - Código de buenas prácticas (en desarrollo).
- **ISO 27799:** es una guía vigente desde Junio 2008 y actualizada en Julio 2016 que proporciona directrices para apoyar la interpretación y aplicación en el sector sanitario de la ISO/IEC 27002 en cuanto a la seguridad de la información de salud de los pacientes.

# ANEXO B – Principales Proveedores SaaS - 2017

| Proveedor | Nombre del producto | Industrias aplicables | Tamaño de Empresa | Total de clientes | Opciones de implementación |
|---|---|---|---|---|---|
| **Acumática** | Acumática Cloud ERP | Fabricación, Distribución, Servicios Profesionales, Comercio Minorista, eCommerce, Software y Tecnología, Propiedad Administrativa, sin ánimo de lucro | Pequeña y Mediana Empresa | 2500+ | SaaS multiusuario,<br>Alojado por un partner<br>Alojado por el proveedor<br>On-premises |
| **Deltek** | Costpoint, Vision, Maconomy y Ajera | Gobierno, Aero espacio y Defensa, Ingeniería, Construcción, Salud, Administración, Consultoría IT, Sin ánimo de lucro | Mediana y Grande Empresa | Costpoint 375+<br>Vision 850+<br>Maconomy 100+<br>Ajena 550+ | SaaS Multiusuarios<br>Alojados por un partner<br>Alojados por proveedor<br>On-premises |
| **Epicor** | Epicor Cloud ERP | Fabricación que incluye maquinaria industrial, alta tecnología, dispositivos médicos, metales fabricados, caucho y plásticos | Mediana Empresa | 550 | SaaS Multiusuario<br>Alojada<br>Hibrida |

| Proveedor | Nombre del producto | Industrias aplicables | Tamaño de Empresa | Total de clientes | Opciones de implementación |
|---|---|---|---|---|---|
| | | | | | On-premises |
| **FinancialForce** | FinancialForce ERP | Servicios de Negocios, Servicios Profesionales, Salud, Servicios Financieros, Medios de Comunicación, Sin ánimo de lucro, Sector Público | Pequeña, Mediana y Grande empresa | 900+ | SaaS multiusuario |
| **Infor** | Familia de productos de Infor CloudSuite (Syteline, M3, Lawson y LN) | Fabricación (alimentos, bebidas, moda, automotriz,, maquinaria industrial, aeroespacial y defensa), Salud, Servicios Profesionales, Distribución al por mayor, Renta de vehículos, Servicios Financieros, Sector Público, Hospitalidad y Venta al por menor | Mediana y Grande empresa | 750+ | SaaS multiusuario<br>Alojada por el partner<br>On-premises |
| **Intacct** | Intacct | Software, Servicios Profesionales, Sin ánimo de lucro, Servicios Financieros, Hospitalidad, Salud, Distribución al por mayor | Pequeña y Mediana Empresa | 11000+ | SaaS Multiusuarios |
| **Kenandy** | Kenandy Cloud ERP | Proceso de Fabricación, Fabricación Discreta, Distribución, CPG, Dispositivos Médicos | Mediana y Grande Empresa | No revelado | SaaS Multiusuario |
| **Microsoft** | Microsoft Dynamics 365 para Operaciones | Fabricación, Venta al por menor, Sector Público, Distribución, Servicios de Industrias, Otras Industrias | Mediana y Grande Empresa | No revelado | Saas alojado en la nube de Microsoft (Azure) |

| Proveedor | Nombre del producto | Industrias aplicables | Tamaño de Empresa | Total de clientes | Opciones de implementación |
|---|---|---|---|---|---|
| | Microsoft Dynamics 365 para Financieros | | | | Hibrido/On-premises |
| **Oracle NetSuite** | NetSuite ERP | Software/Alta Tecnología, Venta al por menor, Fabricación, Sin ánimo de lucro, Distribución al por mayor, Publicidad, Medios y Publicación, Servicios de Industrias | Pequeña, Mediana y Divisiones de Grandes Empresas | 10000+ | SaaS Multiusuario |
| **Oracle** | Oracle ERP Cloud | Servicios Profesionales, Servicios Financieros, Alta Tecnología, Ventas al por menor, Educación e Investigación, Sector Público, Salud | Mediana y Grande Empresa | 2800+ | SaaS<br>Máquina Virtual en la Nube<br>On-premises |
| **Plex Systems** | Plex Manufacturing Cloud | Industrias con procesos de Fabricación | Mediana y Grande Empresa | 500+ | SaaS Multiusuario |
| **QAD** | QAD Cloud ERP | Fabricación incluido automóviles, Ciencias de la Vida, Industrial, Alta Tecnología, Productos de Consumo, Alimentos y Bebidas | Mediana y Grande Empresa | 200+ | Licenciamiento simple en nube<br>On-premises<br>Algunos componentes SaaS |

| Proveedor | Nombre del producto | Industrias aplicables | Tamaño de Empresa | Total de clientes | Opciones de implementación |
|---|---|---|---|---|---|
| **Ramco Systems** | Ramco ERP en nube | Logística, Fabricación, Servicios Profesionales, Gestión de Instalaciones, Alquiler de Equipos y Servicios, Infraestructura y Bienes Inmuebles, Ingeniería y Construcción, Ventas al por menor, Comercio, Banca y Servicios Financieros, Energía | Mediana y Grande Empresa | 400+ | Saas Multiusuario<br>Licenciamiento simple<br>On-premises |
| **Rootstock Software** | Rootstock Cloud ERP para Fabricación, Distribución y Cadena Suministro | Fabricación, Alta Tecnología, Equipamiento Industrial, Maquinaria, Electrónica, Tiendas de Trabajo, Ingeniería, Medicina, Distribución | Pequeña y Mediana Empresa | 100+ | Multiusuario SaaS |
| **SAP** | SAP S/4Hana Cloud<br>SAP Business ByDesign<br>SAP Business One Cloud | Soporta una amplia variedad de industrias con cada producto | Mediana y Grande Empresa (S/4Hana)<br>Mediana Empresa (Business ByDesign)<br>Pequeña Empresa (Business One) | S/4Hana no revelados<br>ByDesign 3500<br>Business One Cloud 2000+ | S/4 Saas Multiusuario, Licenciamiento simple alojado por SAP o Partners<br>On-Premises<br>ByDesign – SaaS Multiusuario<br>Business One – SaaS Multiusuario alojado por SAP o Partners |

| Proveedor | Nombre del producto | Industrias aplicables | Tamaño de Empresa | Total de clientes | Opciones de implementación |
|---|---|---|---|---|---|
| | | | | | On-Premises |
| **Unit4** | Unit4 Business World On | Servicios Profesionales, Servicios Públicos, Sin ánimo de lucro, Educación | Mediana y Grande Empresa | 412 | SaaS Multiusuario<br>On-Premises |
| **Workday** | Workday Financial Management | Educación, Gobierno, Sin ánimo de lucro, Salud, Servicios Profesionales, Servicios de Negocios, Servicios Financieros, Software y Tecnología, Ventas al por menor | Mediana y Grande Empresa | 250+ | SaaS Multiusuario |

# ANEXO C - Inventario de Activos de Información de la Empresa Desarrolladora de Software

| Identificación, Valoración y Clasificación de los Activos de Información | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **N°** | **Activo** | **Tipo de activo** | **Responsable** | **Custodio** | **Confidencialidad** | **Disponibilidad** | **Integridad** | **Valor** | **Importancia** |
| 1 | Dispositivo de Respaldo | Hardware | Dirección | Dirección | 4 | 4 | 5 | 5 | Alto |
| 2 | Impresora | Hardware | Dpto. Administrativo | Dirección | 3 | 3 | 3 | 3 | Bajo |
| 3 | Computador Desarrolladores | Hardware | Dpto. Desarrollo | Dpto. Desarrollo | 4 | 5 | 5 | 4 | Medio |
| 4 | Router de Internet | Hardware | Dpto. Administrativo | Dirección | 3 | 6 | 5 | 5 | Alto |

| Identificación, Valoración y Clasificación de los Activos de Información | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **N°** | **Activo** | **Tipo de activo** | **Responsable** | **Custodio** | **Confidencialidad** | **Disponibilidad** | **Integridad** | **Valor** | **Importancia** |
| 5 | Red Inalámbrica | Hardware | Dpto. Administrativo | Dirección | 3 | 4 | 5 | 3 | Bajo |
| 6 | Internet | Servicio | Proveedor | Dirección | 3 | 5 | 5 | 4 | Medio |
| 7 | Antivirus | Software | Dirección | Dirección | 3 | 4 | 4 | 3 | Bajo |
| 8 | Correo Electrónico Corporativo | Software | Dirección | Dirección | 5 | 5 | 5 | 5 | Alto |
| 9 | Documentación | Información | Dirección | Dirección | 3 | 3 | 5 | 3 | Bajo |
| 10 | Portal Web | Servicio | Proveedor | Dirección | 4 | 6 | 6 | 5 | Alto |
| 11 | Sistema Operativo de Servidores | Software | Dirección | Dirección | 3 | 4 | 5 | 5 | Alto |

| Identificación, Valoración y Clasificación de los Activos de Información | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **N°** | **Activo** | **Tipo de activo** | **Responsable** | **Custodio** | **Confidencialidad** | **Disponibilidad** | **Integridad** | **Valor** | **Importancia** |
| 12 | Motor de Base de Datos | Software | Dpto. Desarrollo | Dirección | 4 | 5 | 5 | 5 | Alto |
| 13 | Bitácora de Actualizaciones | Información | Dirección | Dirección | 3 | 3 | 3 | 3 | Bajo |
| 14 | Manuales de usuarios | Información | Dirección | Dirección | 2 | 2 | 3 | 3 | Bajo |
| 15 | Manuales de Actividades | Información | Dpto. Desarrollo | Dirección | 3 | 4 | 4 | 3 | Bajo |
| 16 | Manuales de estados del aplicativo | Información | Dpto. Desarrollo | Dirección | 3 | 4 | 4 | 4 | Medio |

| Identificación, Valoración y Clasificación de los Activos de Información | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **N°** | **Activo** | **Tipo de activo** | **Responsable** | **Custodio** | **Confidencialidad** | **Disponibilidad** | **Integridad** | **Valor** | **Importancia** |
| 17 | Manual de Recuperación del Servicio | Información | Dirección | Dirección | 4 | 5 | 5 | 5 | Alto |
| 18 | Bitácora de Mantenimientos | Información | Dirección | Dirección | 3 | 3 | 3 | 3 | Bajo |
| 19 | Desarrolladores | Recurso Humano | Dirección | Dirección | 5 | 5 | 5 | 5 | Alto |
| 20 | Proveedores | Recurso Humano | Dirección | Dirección | 5 | 5 | 5 | 5 | Alto |
| 21 | Servicios Cloud | Servicio | Proveedor | Dirección | 4 | 6 | 6 | 5 | Alto |

# ANEXO D - Identificación de Amenazas

| N° | Riesgo | Amenaza | Vulnerabilidad | Tipo de Amenaza | Tipo de Riesgo |
|---|---|---|---|---|---|
| 1 | Interrupción en la Conectividad | Equipos de red lentos | Falta de Mantenimiento | Accidental | Residual |
| 2 | Interrupción en la Conectividad | Falla en las comunicaciones | Equipos obsoletos | Accidental | Residual |
| 3 | Afectación de todos los servicios | Fallo en la red eléctrica | Corte de la alimentación eléctrica | Accidental | Residual |
| 4 | Afectación de todos los servicios | Degradación en los servicios | Caída de servicios por agotamiento de recursos | Accidental | Residual |
| 5 | Afectación a la Reputación Institucional | Errores en el desarrollo del software | Personal no capacitado | Accidental | Residual |
| 6 | Afectación al funcionamiento de los servicios | Modificación de software | Falta de procedimiento de control de cambios | Accidental | Residual |

| N° | Riesgo | Amenaza | Vulnerabilidad | Tipo de Amenaza | Tipo de Riesgo |
|---|---|---|---|---|---|
| 7 | Afectación a la Seguridad de la información | Cambios no autorizados en software | Falta de control de acceso | Accidental | Residual |
| 8 | Afectación a la Seguridad de la información | Ingeniería Social | Suplantación de IP que brinda el servicio | Accidental | Residual |
| 9 | Afectación a la Productividad de la organización | Falla en los servicios de internet | Falta de redundancia de conectividad | Accidental | Residual |
| 10 | Afectación a la Seguridad de la documentación | Modificación de la información | Falta de procedimientos para control de versiones | Accidental | Residual |
| 11 | Afectación a la Seguridad de la información | Información desactualizada | Carencia de Capacitación | Accidental | Residual |
| 12 | Afectación a la disponibilidad de los servicios | Degradación de los servicios | Consumo excesivo de los recursos | Accidental | Residual |
| 13 | Afectación al funcionamiento de los servicios | El sistema se torna lento | Denegación de servicios | Deliberado | Residual |

| N° | Riesgo | Amenaza | Vulnerabilidad | Tipo de Amenaza | Tipo de Riesgo |
|---|---|---|---|---|---|
| 14 | Afectación a la integridad de la información | Suplantación de la identidad de un usuario | Claves débiles | Deliberado | Residual |
| 15 | Afectación en el funcionamiento de los equipos de los usuarios | Manipulación de equipos | Virus | Deliberado | Residual |
| 16 | Afectación a la reputación de la organización | Hackeo | Software mal configurado | Deliberado | Residual |
| 17 | Afectación en el funcionamiento de los servicios | Errores de configuración | Administración de configuración inadecuada | Deliberado | Residual |
| 18 | Afectación al funcionamiento de los servicios | Alteración de información | Software de base de datos desactualizado | Deliberado | Residual |
| 19 | Afectación a la Seguridad de la información | Robo | Oficinas sin monitoreo y vigilancia | Deliberado | Residual |
| 20 | Afectación a la productividad de la organización | Código Malicioso | Descarga y uso de software de Internet no controlada | Deliberado | Residual |

| N° | Riesgo | Amenaza | Vulnerabilidad | Tipo de Amenaza | Tipo de Riesgo |
|---|---|---|---|---|---|
| 21 | Afectación a la Seguridad de la Información | Fuga de información | Acceso no autorizado | Deliberado | Residual |
| 22 | Afectación a la Seguridad de la información | Espionaje | Abuso de conocimientos internos | Deliberado | Residual |
| 23 | Afectación al funcionamiento de los servicios | Degradación de los servicios | Carencia de Firewall | Deliberado | Residual |
| 24 | Afectación a la Seguridad de la información | Robo | Perdida de equipos | Deliberado | Inherente |
| 25 | Afectación a la Seguridad de la información | Uso de información del sistema para fines Personales/Delictivos | Acceso no autorizado | Deliberado | Inherente |
| 26 | Interrupción a la Integridad de la Información | Modificación deliberada de información | Corrupción de Base de Datos | Deliberado | Inherente |

| N° | Riesgo | Amenaza | Vulnerabilidad | Tipo de Amenaza | Tipo de Riesgo |
|---|---|---|---|---|---|
| 27 | Afectación a la Seguridad de la Información | Extorsión | Persona con información sensible | Deliberado | Inherente |
| 28 | Interrupción de la disponibilidad de los servicios | Desastres Naturales | Sismo | Entorno | Residual |
| 29 | Interrupción de la disponibilidad de los servicios | Fuego | Cables cortados o quemados | Entorno | Inherente |

# ANEXO E - MATRIZ DE RIESGOS

| MATRIZ DE RIESGOS | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Identificación de Amenazas y Valoración del Riesgo** | | | | | | | | | | | |
| **N°** | **Tipo** | **Activo** | **Valor** | **Tipo de Amenaza** | **Tipo de Riesgo** | **Riesgo** | **Amenaza** | **Vulnerabilidad** | **Probabilidad** | **Impacto** | **Impacto-Consecuencia** |
| 1 | Hardware | Red Wan | 5 | Accidental | Residual | Interrupción en la Conectividad | Equipos de red lentos | Falta de Mantenimiento | 5 | 5 | Extremo |
| 2 | Hardware | Red Wan | 5 | Accidental | Residual | Interrupción en la Conectividad | Falla en las comunicaciones | Equipos obsoletos | 3 | 3 | Alto |
| 3 | Hardware | Instalaciones | 5 | Accidental | Residual | Afectación de todos los servicios | Fallo en la red eléctrica | Corte de la alimentación eléctrica | 5 | 3 | Extremo |
| 4 | Hardware | Servidores | 5 | Accidental | Residual | Afectación de todos los servicios | Degradación en los servicios | Caída de servicios por agotamiento de recursos | 4 | 3 | Alto |

## MATRIZ DE RIESGOS

### Identificación de Amenazas y Valoración del Riesgo

| N° | Tipo | Activo | Valor | Tipo de Amenaza | Tipo de Riesgo | Riesgo | Amenaza | Vulnerabilidad | Probabilidad | Impacto | Impacto-Consecuencia |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 5 | Software | Código Fuente | 3 | Accidental | Residual | Afectación a la Reputación Institucional | Errores en el desarrollo del software | Personal no capacitado | 3 | 4 | Extremo |
| **6** | Software | Aplicaciones Documental | 5 | Accidental | Residual | Afectación al funcionamiento de los servicios | Modificación de software | Falta de procedimiento de control de cambios | 2 | 4 | Extremo |
| **7** | Software | Aplicaciones Documental | 5 | Accidental | Residual | Afectación a la Seguridad de la información | Cambios no autorizados en software | Falta de control de acceso | 2 | 2 | Bajo |
| **8** | Redes | Red LAN | 4 | Accidental | Residual | Afectación a la Seguridad de la información | Ingeniería Social | Suplantación de IP que brinda el servicio | 5 | 2 | Alto |

## MATRIZ DE RIESGOS

### Identificación de Amenazas y Valoración del Riesgo

| N° | Tipo | Activo | Valor | Tipo de Amenaza | Tipo de Riesgo | Riesgo | Amenaza | Vulnerabilidad | Probabilidad | Impacto | Impacto-Consecuencia |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **9** | Redes | Internet | 4 | Accidental | Residual | Afectación a la Productividad de la organización | Falla en los servicios de internet | Falta de redundancia de conectividad | 2 | 3 | Moderado |
| **10** | Información | Manuales | 4 | Accidental | Residual | Afectación a la Seguridad de la documentación | Modificación de la información | Falta de procedimientos para control de versiones | 2 | 3 | Moderado |
| **11** | Información | Política de Seguridad | 3 | Accidental | Residual | Afectación a la Seguridad de la información | Información desactualizada | Carencia de Capacitación | 2 | 4 | Alto |
| **12** | Software | Servidores Virtuales | 5 | Accidental | Residual | Afectación a la disponibilidad de los servicios | Degradación de los servicios | Consumo excesivo de los recursos | 4 | 3 | Alto |

## MATRIZ DE RIESGOS

## Identificación de Amenazas y Valoración del Riesgo

| N° | Tipo | Activo | Valor | Tipo de Amenaza | Tipo de Riesgo | Riesgo | Amenaza | Vulnerabilidad | Probabilidad | Impacto | Impacto-Consecuencia |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **13** | Hardware | Firewall | 5 | Deliberado | Residual | Afectación al funcionamiento de los servicios | El sistema se torna lento | Denegación de servicios | 4 | 4 | Extremo |
| **14** | Software | Correo Electrónico Corporativo | 5 | Deliberado | Residual | Afectación a la integridad de la información | Suplantación de la identidad de un usuario | Claves débiles | 4 | 3 | Alto |
| **15** | Hardware | Computador Usuario | 3 | Deliberado | Residual | Afectación en el funcionamiento de los equipos de los usuarios | Manipulación de equipos | Virus | 5 | 3 | Extremo |
| **16** | Software | Sitio Web | 4 | Deliberado | Residual | Afectación a la reputación de la organización | Hackeo | Software mal configurado | 2 | 3 | Moderado |

## MATRIZ DE RIESGOS

### Identificación de Amenazas y Valoración del Riesgo

| N° | Tipo | Activo | Valor | Tipo de Amenaza | Tipo de Riesgo | Riesgo | Amenaza | Vulnerabilidad | Probabilidad | Impacto | Impacto-Consecuencia |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **17** | Software | Gestor de Máquinas Virtuales | 5 | Deliberado | Residual | Afectación en el funcionamiento de los servicios | Errores de configuración | Administración de configuración inadecuada | 3 | 4 | Extremo |
| **18** | Software | Motor de Base de Datos | 5 | Deliberado | Residual | Afectación al funcionamiento de los servicios | Alteración de información | Software de base de datos desactualizado | 3 | 4 | Extremo |
| **19** | Hardware | Sistema de Monitoreo | 3 | Deliberado | Residual | Afectación a la Seguridad de la información | Robo | Oficinas sin monitoreo y vigilancia | 2 | 2 | Bajo |
| **20** | Hardware | Firewall LAN | 5 | Deliberado | Residual | Afectación a la productividad de la organización | Código Malicioso | Descarga y uso de software de Internet no controlada | 3 | 3 | Alto |

## MATRIZ DE RIESGOS

### Identificación de Amenazas y Valoración del Riesgo

| N° | Tipo | Activo | Valor | Tipo de Amenaza | Tipo de Riesgo | Riesgo | Amenaza | Vulnerabilidad | Probabilidad | Impacto | Impacto-Consecuencia |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **21** | Información | Requerimientos | 3 | Deliberado | Residual | Afectación a la Seguridad de la Información | Fuga de información | Acceso no autorizado | 2 | 4 | Alto |
| **22** | Recurso Humano | Dirección | 5 | Deliberado | Residual | Afectación a la Seguridad de la información | Espionaje | Abuso de conocimientos internos | 1 | 4 | Alto |
| **23** | Servicio | Sistema de Resolución de Nombres | 5 | Deliberado | Residual | Afectación al funcionamiento de los servicios | Degradación de los servicios | Carencia de Firewall | 3 | 3 | Alto |
| **24** | Firewall de Red LAN | Hardware | 5 | Deliberado | Inherente | Afectación a la Seguridad de la información | Robo | Perdida de equipos | 1 | 4 | Alto |
| **25** | Sistema | Software | 5 | Deliberado | Inherente | Afectación a la Seguridad de la información | Uso de información del sistema para fines Personales/Delictivos | Acceso no autorizado | 1 | 3 | Moderado |

# MATRIZ DE RIESGOS

## Identificación de Amenazas y Valoración del Riesgo

| N° | Tipo | Activo | Valor | Tipo de Amenaza | Tipo de Riesgo | Riesgo | Amenaza | Vulnerabilidad | Probabilidad | Impacto | Impacto-Consecuencia |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **26** | Base de Datos | Software | 5 | Deliberado | Inherente | Interrupción a la Integridad de la Información | Modificación deliberada de información | Corrupción de Base de Datos | 1 | 4 | Alto |
| **27** | Administrador | Recurso Humano | 5 | Deliberado | Inherente | Afectación a la Seguridad de la Información | Extorsión | Persona con información sensible | 1 | 3 | Moderado |
| **28** | Hardware | Data Center | 5 | Entorno | Residual | Interrupción de la disponibilidad de los servicios | Desastres Naturales | Sismo | 1 | 5 | Extremo |
| **29** | Data Center | Instalaciones | 5 | Entorno | Inherente | Interrupción de la disponibilidad de los servicios | Fuego | Cables cortados o quemados | 1 | 1 | Extremo |

# ANEXO F – PLAN DE TRATAMIENTO DE RIESGOS

# ANEXO G – ASIGNACION DE CONTROLES

| TRATAMIENTO DE RIESGO | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Riesgo** | **Amenaza** | **Vulnerabilidad** | **Acción tratamiento** | **Proyecto/Actividad** | **Controles** | **Descripción del Control** | **Responsable** | **Registro** |
| Interrupción en la Conectividad | Equipos de red lentos | Falta de Mantenimiento | Reducir | Implementación de un Proveedor de Servicios Cloud de Contingencia | A.17.2 Redundancias | Equipos configurados en alta disponibilidad evitando afectar la continuidad del negocio | Dirección | Implementación de un Proveedor de Servicios Cloud de Contingencia |
| | | | | | A.11.2.4 Mantenimiento de Equipos | Mantenimiento correcto de los equipos asegurando integridad y disponibilidad. | | |
| | Falla en las comunicaciones | Equipos obsoletos | Evitar | | A.17.2 Redundancias | Equipos configurados en alta disponibilidad evitando afectar la | Dirección | |

| TRATAMIENTO DE RIESGO | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Riesgo** | **Amenaza** | **Vulnerabilidad** | **Acción tratamiento** | **Proyecto/Actividad** | **Controles** | **Descripción del Control** | **Responsable** | **Registro** |
| Interrupción en la Conectividad | | | | Actualización físico/lógico de la infraestructura | | continuidad del negocio | | Indicadores de disponibilidad de red |
| | | | | | A.11.2.4 Mantenimiento de Equipos | Mantenimiento correcto de los equipos asegurando integridad y disponibilidad. | | |
| Afectación de todos los servicios | Fallo en la red eléctrica | Corte de la alimentación eléctrica | Evitar | Adquirir Generador | A.11.2.2 Servicios de Suministros | Defender contra desperfectos de energía y suspensiones | Dirección | Indicadores de fallas de energía |
| | | | | | A.17.2 Redundancia | Contingencia contra defectos de energía. | | |
| | | | | | A.12.1.3 Gestión de Capacidad | Desarrollar rastreo a la utilización de | | |

| TRATAMIENTO DE RIESGO | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Riesgo** | **Amenaza** | **Vulnerabilidad** | **Acción tratamiento** | **Proyecto/Actividad** | **Controles** | **Descripción del Control** | **Responsable** | **Registro** |
| | | | | | | recursos, para proceder con importancia a los mantenimientos reparaciones o cambios. | | |
| Afectación de todos los servicios | Degradación en los servicios | Caída de servicios por agotamiento de recursos | Evitar | Implementación de un Proveedor de Servicios Cloud de Contingencia | A.17.2 Redundancias | Equipos configurados en alta disponibilidad evitando afectar la continuidad del negocio | Dirección | Implementación de un Proveedor de Servicios Cloud de Contingencia |
| | | | | | A.11.2.4 Mantenimiento de Equipos | Mantenimiento correcto de los equipos asegurando integridad y disponibilidad. | | |

| TRATAMIENTO DE RIESGO | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Riesgo** | **Amenaza** | **Vulnerabilidad** | **Acción tratamiento** | **Proyecto/Actividad** | **Controles** | **Descripción del Control** | **Responsable** | **Registro** |
| Afectación a la Reputación Institucional | Errores en el desarrollo del software | Personal no capacitado | Evitar | Capacitación especializada constante al personal | A.13.2.1 Políticas y Procedimientos de transferencia de información | Se debe proteger la transferencia de la información con políticas, controles o procedimientos. | Dirección | Reporte de capacitación al personal |
| | | | | | A.14.2.1 Política de desarrollo seguro | Asignar y crear reglas que apliquen para el desarrollo del software. | | |
| | | | | | A.14.2.2 Procedimientos de control de cambios en sistemas | Comprobar que los cambios realizados a los sistemas estén considerados en el ciclo de vida de desarrollo. | | |

| TRATAMIENTO DE RIESGO | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Riesgo** | **Amenaza** | **Vulnerabilidad** | **Acción tratamiento** | **Proyecto/Actividad** | **Controles** | **Descripción del Control** | **Responsable** | **Registro** |
| | | | | | A.14.2.9 Prueba de aceptación de sistemas | Constituir criterios de prueba para aceptar las actualizaciones y versiones nuevas. | | |
| Afectación al funcionamiento de los servicios | Modificación de software | Falta de procedimiento de control de cambios | Evitar | Actualización del Plan de Continuidad del negocio | A.13.2.1 Políticas y procedimientos de transferencia de información | Se debe proteger la transferencia de la información con políticas, controles o procedimientos | Dirección | Reporte de registro de documentos |
| | | | | | A.12.1.2 Administración de los cambios | Administrar los cambios realizados sobre las instalaciones y sistemas de procesamiento de la información. | | |

| TRATAMIENTO DE RIESGO | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Riesgo** | **Amenaza** | **Vulnerabilidad** | **Acción tratamiento** | **Proyecto/Actividad** | **Controles** | **Descripción del Control** | **Responsable** | **Registro** |
| | | | | | A.14.2.2 Procedimientos de control de cambios en sistemas | Comprobar que los cambios realizados a los sistemas estén considerados en el ciclo de vida de desarrollo. | | |
| Afectación a la Seguridad de la información | Cambios no autorizados en software | Falta de control de acceso | Evitar | Implementación de un Proveedor de Servicios Cloud de Contingencia | A.14.1.2 Seguridad de servicios de las aplicaciones | Resguardar que no se cometan actividades fraudulentas como la divulgación y modificación no autorizadas. | Dpto. Desarrollo | Reporte de monitoreo de servicio |
| | | | | | A.17.2 Redundancias | Equipos configurados en alta disponibilidad evitando afectar la | | |

| TRATAMIENTO DE RIESGO | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Riesgo** | **Amenaza** | **Vulnerabilidad** | **Acción tratamiento** | **Proyecto/Actividad** | **Controles** | **Descripción del Control** | **Responsable** | **Registro** |
| | | | | | | continuidad del negocio | | |
| | | | | | A.12.3.1 Protección de la información | Proteger la información, software e imágenes de los sistemas y verificarlas periódicamente. | | |
| Afectación a la Seguridad de la información | Ingeniería Social | Suplantación de IP que brinda el servicio | Evitar | Capacitación especializada constante al personal | A.12.4.2 Defensa de la información | Asegurar las instalaciones, recursos e información contra la modificación y el acceso inadecuado. | Dirección | Indicadores de capacitación |
| | | | | | A.7.2.2 Adquisición de conocimiento,, educación y formación | Se debe brindar una correcta educación y formación apropiada | | |

| TRATAMIENTO DE RIESGO | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Riesgo** | **Amenaza** | **Vulnerabilidad** | **Acción tratamiento** | **Proyecto/Actividad** | **Controles** | **Descripción del Control** | **Responsable** | **Registro** |
| | | | | | en la seguridad de la información | para una correcta toma de conciencia en cuanto a la seguridad de la información | | |
| | | | | | A.16.1.1 Responsabilidades y Procedimientos | Establecer obligaciones y métodos para soluciones rápidas, eficaces y ordenadas a los eventos de seguridad de la información | | |
| Afectación a la Productividad | Falla en los servicios de internet | | Evitar | | A.17.2 Redundancias | Equipos configurados en alta disponibilidad evitando afectar la | Dirección | |

| TRATAMIENTO DE RIESGO | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Riesgo** | **Amenaza** | **Vulnerabilidad** | **Acción tratamiento** | **Proyecto/Actividad** | **Controles** | **Descripción del Control** | **Responsable** | **Registro** |
| de la organización | | Falta de redundancia de conectividad | | Actualización físico/lógico de la infraestructura | | continuidad del negocio. | | Reporte de Estados de Servicios |
| | | | | | A.15.2.1 Seguimiento y revisión de los servicios de los proveedores | Todo servicio prestado por proveedores debe ser verificado y auditado con regularidad. | | |
| Afectación a la Seguridad de la documentación | Modificación de la información | Falta de procedimientos para control de versiones | Evitar | Actualización del Plan de Continuidad del negocio | A.12.1.2 Administración de los cambios | Administrar los cambios realizados sobre las instalaciones y sistemas de procesamiento de la información. | Dirección | Registro de procedimientos |

| TRATAMIENTO DE RIESGO | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Riesgo** | **Amenaza** | **Vulnerabilidad** | **Acción tratamiento** | **Proyecto/Actividad** | **Controles** | **Descripción del Control** | **Responsable** | **Registro** |
| Afectación a la Seguridad de la información | Información desactualizada | Carencia de Capacitación | Evitar | Capacitación especializada constante al personal | A.12.1.2 Administración de los cambios | Administrar los cambios realizados sobre las instalaciones y sistemas de procesamiento de la información. | Dirección | Indicadores de capacitación |
| | | | | | A.13.2.1 Políticas y procedimientos de transferencia de información | Se debe proteger la transferencia de la información con políticas, controles o procedimientos. | | |
| Afectación a la disponibilidad | Degradación de los servicios | Consumo excesivo de los recursos | Reducir | Actualización físico/lógico de la infraestructura | A.12.1.3 Gestión de capacidad | Desarrollar rastreo a la utilización de recursos, para proceder con | Dirección | Reporte de estado de servicio |

| TRATAMIENTO DE RIESGO | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Riesgo** | **Amenaza** | **Vulnerabilidad** | **Acción tratamiento** | **Proyecto/Actividad** | **Controles** | **Descripción del Control** | **Responsable** | **Registro** |
| de los servicios | | | | | | importancia a los mantenimientos reparaciones o cambios. | | |
| | | | | | A.12.6.1 Administración de las vulnerabilidades técnicas | Verificar las vulnerabilidades técnicas de los sistemas; evaluándolos y tomando las medidas necesarias. | | |
| | | | | | A.12.1.2 Administración de los cambios | Administrar los cambios realizados sobre las instalaciones y sistemas de | | |

| TRATAMIENTO DE RIESGO | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Riesgo** | **Amenaza** | **Vulnerabilidad** | **Acción tratamiento** | **Proyecto/Actividad** | **Controles** | **Descripción del Control** | **Responsable** | **Registro** |
| | | | | | | procesamiento de la información. | | |
| Afectación al funcionamiento de los servicios | El sistema se torna lento | Denegación de servicios | Evitar | Implementación de un Proveedor de Servicios Cloud de Contingencia | A.11.2.4 Mantenimiento de equipos | Mantenimiento correcto de los equipos asegurando integridad y disponibilidad. | Dirección | Reporte de estado de seguridad de la información |
| | | | | | A.17.2 Redundancias | Equipos configurados en alta disponibilidad evitando afectar la continuidad del negocio. | | |
| | | | | | A.12.1.3 Gestión de capacidad | Desarrollar rastreo a la utilización de recursos, para proceder con | | |

| TRATAMIENTO DE RIESGO | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Riesgo** | **Amenaza** | **Vulnerabilidad** | **Acción tratamiento** | **Proyecto/Actividad** | **Controles** | **Descripción del Control** | **Responsable** | **Registro** |
| | | | | | | importancia a los mantenimientos reparaciones o cambios. | | |
| | | | | | A.13.1.2 Seguridad de los servicios de red | Reconocimiento a los mecanismos de seguridad y a los niveles de servicios de la red. | | |
| Afectación a la integridad de la información | Suplantación de la identidad de un usuario | Claves débiles | Evitar | Capacitación especializada constante al personal | A.7.2.1 Aplicación de la Seguridad de la información para empleados y contratistas | Requerir por parte de los usuarios el cumplimiento de la política de seguridad, con el fin de evitar que las contraseñas sean débiles arriesgando el | Dirección | Entrenamiento especializado a personal |

| TRATAMIENTO DE RIESGO | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Riesgo** | **Amenaza** | **Vulnerabilidad** | **Acción tratamiento** | **Proyecto/Actividad** | **Controles** | **Descripción del Control** | **Responsable** | **Registro** |
| | | | | | | ingreso de cuentas institucionales. | | |
| | | | | | A.9.2.3 Administración de derechos de acceso privilegiado | Se debe realizar chequeos periódicos a los accesos otorgados a los usuarios con el fin de impedir el acceso sin autorización y el uso inadecuado de los permisos otorgados. | | |
| | | | | | A.9.4.3 Sistema de gestión de contraseñas | Se debe implementar un sistema de gestión de contraseñas interactivo y dinámico para asegurar la | | |

| TRATAMIENTO DE RIESGO | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Riesgo** | **Amenaza** | **Vulnerabilidad** | **Acción tratamiento** | **Proyecto/Actividad** | **Controles** | **Descripción del Control** | **Responsable** | **Registro** |
| | | | | | | calidad de las contraseñas. | | |
| | | | | | A.9.3.1 Uso de información de autenticación secreta | Requerir por parte de los usuarios el cumplimiento de las medidas de seguridad sobre el uso de autenticación secreta. | | |
| Afectación en el funcionamiento de los equipos de los usuarios | Manipulación de equipos | Virus | Evitar | Asignación de responsabilidades de seguridad de la información | A.12.2.1 Controles contra códigos maliciosos | Hacer uso de controles para ayudar a la detección, prevención y eliminación de código malicioso, al igual que procedimientos de | Responsable de Seguridad de la Información | Reporte de estado de seguridad de la información |

| TRATAMIENTO DE RIESGO | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Riesgo** | **Amenaza** | **Vulnerabilidad** | **Acción tratamiento** | **Proyecto/Actividad** | **Controles** | **Descripción del Control** | **Responsable** | **Registro** |
| | | | | | | recuperación de la información. | | |
| | | | | | A.12.5.1 Instalación de software en sistemas operativos | Realizar la instalación de software en base a procedimientos controlados. | | |
| | | | | | A.16.1.3 Reporte de debilidades de seguridad de la información | Requerir por parte de empleados y contratistas que usan los servicios de la organización, el observar y reportar cualquier debilidad de los sistemas. | | |

| TRATAMIENTO DE RIESGO | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Riesgo** | **Amenaza** | **Vulnerabilidad** | **Acción tratamiento** | **Proyecto/Actividad** | **Controles** | **Descripción del Control** | **Responsable** | **Registro** |
| | | | | | A.18.2.3 Revisión del cumplimiento técnico | Examinar con periodicidad el cumplimiento de los sistemas de información. | | |
| Afectación a la reputación de la organización | Hackeo | Software mal configurado | Evitar | Asignación de responsabilidades de seguridad de la información | A.12.4.2 Defensa de la información | Asegurar las instalaciones, recursos e información contra la modificación y el acceso inadecuado. | Responsable de Seguridad de la Información | Indicadores de Seguridad de la información |
| | | | | | A.12.6.1 Administración de las vulnerabilidades técnicas | Verificar las vulnerabilidades técnicas de los sistemas; evaluándolos y | | |

| TRATAMIENTO DE RIESGO | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Riesgo** | **Amenaza** | **Vulnerabilidad** | **Acción tratamiento** | **Proyecto/Actividad** | **Controles** | **Descripción del Control** | **Responsable** | **Registro** |
| | | | | | | tomando las medidas necesarias. | | |
| | | | | | A.12.3.1 Protección de la información | Efectuar copias de respaldo de la información en caso de eventos en los equipos | | |
| | | | | | A.16.1.4 Valoración de eventos de seguridad de la información | Se debe evaluar todo evento de seguridad de la información, documentando lo sucedido con el fin de evitar futuros eventos. | | |
| Afectación en el funcionamiento | Errores de configuración | | Evitar | Implementación de un Proveedor de | A.12.1.4 Independencia al manejar los ambientes | Se sugiere la independencia de los ambientes de | Dirección | |

| TRATAMIENTO DE RIESGO | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Riesgo** | **Amenaza** | **Vulnerabilidad** | **Acción tratamiento** | **Proyecto/Actividad** | **Controles** | **Descripción del Control** | **Responsable** | **Registro** |
| de los servicios | | Administración de configuración inadecuada | | Servicios Cloud de Contingencia | de desarrollo, de pruebas y de operaciones | desarrollo, pruebas y operaciones, para reducir los riesgos de acceso o cambios no autorizados al ambiente de producción. | | Reporte de estado de servicio |
| | | | | | A.12.1.2 Administración de los cambios | Administrar los cambios realizados sobre las instalaciones y sistemas de procesamiento de la información. | | |
| | | | | | A.17.2 Redundancias | Equipos configurados en alta disponibilidad | | |

| TRATAMIENTO DE RIESGO | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Riesgo** | **Amenaza** | **Vulnerabilidad** | **Acción tratamiento** | **Proyecto/Actividad** | **Controles** | **Descripción del Control** | **Responsable** | **Registro** |
| | | | | | | evitando afectar la continuidad del negocio. | | |
| | | | | | A.12.3.1 Protección de la información | Efectuar respaldo de la información, software e imágenes de los sistemas y efectuar pruebas periódicamente. | | |
| Afectación al funcionamiento de los servicios | Alteración de información | Software de base de datos desactualizado | Evitar | Actualización físico/lógico de la infraestructura | A.13.2.1 Políticas y procedimientos de transferencia de información | Se debe proteger la transferencia de la información con políticas, controles o procedimientos. | Dirección | Indicadores de estado de servicio |

| TRATAMIENTO DE RIESGO | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Riesgo** | **Amenaza** | **Vulnerabilidad** | **Acción tratamiento** | **Proyecto/Actividad** | **Controles** | **Descripción del Control** | **Responsable** | **Registro** |
| | | | | | A.12.4.2 Defensa de la información | Asegurar las instalaciones, recursos e información contra la modificación y el acceso inadecuado. | | |
| | | | | | A.17.2 Redundancias | Equipos configurados en alta disponibilidad evitando afectar la continuidad del negocio. | | |
| | | | | | A.12.3.1 Protección de la información | Efectuar respaldo de la información,, software e imágenes de los sistemas y | | |

| TRATAMIENTO DE RIESGO | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Riesgo** | **Amenaza** | **Vulnerabilidad** | **Acción tratamiento** | **Proyecto/Actividad** | **Controles** | **Descripción del Control** | **Responsable** | **Registro** |
| | | | | | | realizar pruebas periódicamente | | |
| Afectación a la Seguridad de la información | Robo | Oficinas sin monitoreo y vigilancia | Evitar | Asignación de responsabilidades de seguridad de la información | A.11.1.3 Seguridad de oficinas, recintos e instalaciones | Plantear y utilizar medidas de seguridad física a oficinas e instalaciones | Responsable de Seguridad de la Información | Reporte de accesos a oficina |
| Afectación a la productividad de la organización | Código Malicioso | Descarga y uso de software de Internet no controlada | Evitar | Actualización físico/lógico de la infraestructura | A.17.2 Redundancias | Equipos configurados en alta disponibilidad evitando afectar la continuidad del negocio | Dirección | Indicadores de disponibilidad de equipos de seguridad |
| | | | | | A.12.2.1 Controles contra códigos maliciosos | Implementar controles de detección, de prevención y eliminación de código malicioso, así como | | |

| TRATAMIENTO DE RIESGO | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Riesgo** | **Amenaza** | **Vulnerabilidad** | **Acción tratamiento** | **Proyecto/Actividad** | **Controles** | **Descripción del Control** | **Responsable** | **Registro** |
| | | | | | | controles de recuperación información. | | |
| | | | | | A.12.6.1 Administración de las vulnerabilidades técnicas | Verificar las vulnerabilidades técnicas de los sistemas; evaluándolos y tomando las medidas necesarias | | |
| Afectación a la Seguridad de la Información | Fuga de información | Acceso no autorizado | Evitar | Asignación de responsabilidades de seguridad de la información | A.12.4.2 Defensa de la información | Asegurar las instalaciones, recursos e información contra la modificación y el acceso inadecuado | Responsable de Seguridad de la Información | Registro de procedimientos |

| TRATAMIENTO DE RIESGO | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Riesgo** | **Amenaza** | **Vulnerabilidad** | **Acción tratamiento** | **Proyecto/Actividad** | **Controles** | **Descripción del Control** | **Responsable** | **Registro** |
| | | | | | A.16.1.1 Responsabilidades y Procedimientos | Establecer obligaciones y métodos para soluciones rápidas, eficaces y ordenadas a los eventos de seguridad de la información | | |
| Afectación a la Seguridad de la información | Espionaje | Abuso de conocimientos internos | Reducir | Modernización de equipos de Seguridad de Información | A.16.1.1 Responsabilidades y Procedimientos | Establecer obligaciones y métodos para soluciones rápidas, eficaces y ordenadas a los eventos de seguridad de la información | Responsable de Seguridad de la Información | Registro de procedimientos |

| TRATAMIENTO DE RIESGO | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Riesgo** | **Amenaza** | **Vulnerabilidad** | **Acción tratamiento** | **Proyecto/Actividad** | **Controles** | **Descripción del Control** | **Responsable** | **Registro** |
| | | | | | A.12.1.2 Administración de los cambios | Administrar los cambios realizados sobre las instalaciones y sistemas de procesamiento de la información | | |
| Afectación al funcionamiento de los servicios | Degradación de los servicios | Carencia de Firewall | Evitar | Modernización de equipos de Seguridad de Información | A.12.1.3 Gestión de capacidad | Desarrollar rastreo a la utilización de recursos, para proceder con importancia a los mantenimientos reparaciones o cambios | Responsable de Seguridad de la Información | Reporte de estado de servicio |

| TRATAMIENTO DE RIESGO | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Riesgo** | **Amenaza** | **Vulnerabilidad** | **Acción tratamiento** | **Proyecto/Actividad** | **Controles** | **Descripción del Control** | **Responsable** | **Registro** |
| | | | | | A.12.6.1 Administración de las vulnerabilidades técnicas | Verificar las vulnerabilidades técnicas de los sistemas; evaluándolos y tomando las medidas necesarias | | |
| Afectación a la Seguridad de la información | Robo | Perdida de equipos | Evitar | Modernización de equipos de Seguridad de Información | A.11.1.1 Perímetro de seguridad | Determinar y utilizar cercos de seguridad y acceso con usuarios para proteger áreas con información confidencial o critica | Responsable de Seguridad de la Información | Reporte de estado de Seguridad de Información |
| | | | | | A.11.1.3 Seguridad de oficinas, recintos e instalaciones | Plantear y utilizar medidas de seguridad | | |

| TRATAMIENTO DE RIESGO | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Riesgo** | **Amenaza** | **Vulnerabilidad** | **Acción tratamiento** | **Proyecto/Actividad** | **Controles** | **Descripción del Control** | **Responsable** | **Registro** |
| | | | | | | física a oficinas e instalaciones | | |
| Afectación a la Seguridad de la información | Uso de información del sistema para fines Personales/Delictivos | Acceso no autorizado | Evitar | Modernización de equipos de Seguridad de Información | A.12.4.2 Defensa de la información | Asegurar las instalaciones, recursos e información contra la modificación y el acceso inadecuado | Responsable de Seguridad de la Información | Indicadores de acceso a los servicios |
| | | | | | A.9.2.3 Administración de derechos de acceso privilegiado | Se debe realizar chequeos periódicos a los accesos otorgados a los usuarios con el fin de impedir el acceso sin autorización y el uso | | |

| TRATAMIENTO DE RIESGO | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Riesgo** | **Amenaza** | **Vulnerabilidad** | **Acción tratamiento** | **Proyecto/Actividad** | **Controles** | **Descripción del Control** | **Responsable** | **Registro** |
| | | | | | | inadecuado de los permisos otorgados | | |
| Interrupción a la Integridad de la Información | Modificación deliberada de información | Corrupción de Base de Datos | Evitar | Modernización de equipos de Seguridad de Información | A.12.4.2 Defensa de la información | Asegurar las instalaciones, recursos e información contra la modificación y el acceso inadecuado. | Responsable de Seguridad de la Información | Reporte de estado de Seguridad de la Información |
| | | | | | A.17.2 Redundancias | Equipos configurados en alta disponibilidad evitando afectar la continuidad del negocio | | |
| | | | | | A.12.3.1 Protección de la información | Efectuar respaldo de la información,, software e imágenes | | |

| TRATAMIENTO DE RIESGO | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Riesgo** | **Amenaza** | **Vulnerabilidad** | **Acción tratamiento** | **Proyecto/Actividad** | **Controles** | **Descripción del Control** | **Responsable** | **Registro** |
| | | | | | | de los sistemas y ejecutar pruebas periódicamente | | |
| | | | | | A.17.1.2 Implantación de continuidad de la seguridad de la información | Implantación de sitio alterno para los Sistemas Críticos garantizando la continuidad de las operaciones | | |
| Afectación a la Seguridad de la Información | Extorsión | Persona con información sensible | Reducir | Capacitación especializada constante al personal | A.16.1.1 Responsabilidades y Procedimientos | Establecer obligaciones y métodos para soluciones rápidas, eficaces y ordenadas a los eventos de | Dirección | Reporte de Capacitaciones |

| TRATAMIENTO DE RIESGO | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Riesgo** | **Amenaza** | **Vulnerabilidad** | **Acción tratamiento** | **Proyecto/Actividad** | **Controles** | **Descripción del Control** | **Responsable** | **Registro** |
| | | | | | | seguridad de la información | | |
| | | | | | A.15.1.1 Manejo de normas de Seguridad de la Información para Proveedores | Acuerdo de confidencialidad documentado con los proveedores, sobre la forma de tratar, divulgar y usar la información | | |
| | | | | | A.12.1.2 Administración de los cambios | Administrar los cambios realizados sobre las instalaciones y sistemas de procesamiento de la información | | |

| TRATAMIENTO DE RIESGO | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Riesgo** | **Amenaza** | **Vulnerabilidad** | **Acción tratamiento** | **Proyecto/Actividad** | **Controles** | **Descripción del Control** | **Responsable** | **Registro** |
| Interrupción de la disponibilidad de los servicios | Desastres Naturales | Sismo | Evitar | Implementación de un Proveedor de Servicios Cloud de Contingencia | A.16.1.1 Responsabilidades y Procedimientos | Establecer responsabilidades y procedimientos para respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información. | Dirección | Indicadores de disponibilidad de servicio |
| | | | | | A.17.1.2 Implementación de continuidad de la seguridad de la información | Implementación de sitio alterno. | | |
| Interrupción de la disponibilidad | Fuego | Cables cortados o quemados | Evitar | Actualización físico/lógico de la infraestructura | A.5.1 Realización de Política de Seguridad de Información | Realizar política para la seguridad de la información que | Dirección | Indicadores de disponibilidad del servicio |

| TRATAMIENTO DE RIESGO | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Riesgo** | **Amenaza** | **Vulnerabilidad** | **Acción tratamiento** | **Proyecto/Actividad** | **Controles** | **Descripción del Control** | **Responsable** | **Registro** |
| de los servicios | | | | | | describa los lineamientos para procedimiento en caso de desastres naturales | | |
| | | | | | A.11.1.4 Defensa ante amenazas externas y ambientales | Realizar procedimiento para seguridad física contra eventos naturales, ataques malintencionados o accidentes | | |
| | | | | | A.16.1.5 Solución a eventos de seguridad de la información | Recursos para respuesta ante eventos | | |

# ANEXO H – DECLARACION DE APLICABILIDAD

| DECLARACION DE APLICABILIDAD | | | | |
|---|---|---|---|---|
| **Sección** | **Dominio, Objetivo de Control y controles** | **Aplicabilidad** | **Justificación** | **Recomendación** |
| **A.5.** | **Políticas de Seguridad de la Información** | | | |
| **A. 5.1** | **Disposición de la dirección para la gestión de la seguridad de la información** | | | |
| A.5.1.1 | Políticas para la seguridad de la información | Aplica | Difusión mensual a través de correo electrónico | |
| A.5.1.2 | Revisión de las Políticas para la seguridad de la información | Aplica | Revisión y Actualización anual | |
| **A.7.** | **Seguridad relativa a los Recursos Humanos** | | | |

| DECLARACION DE APLICABILIDAD | | | | |
|---|---|---|---|---|
| **Sección** | **Dominio, Objetivo de Control y controles** | **Aplicabilidad** | **Justificación** | **Recomendación** |
| **A. 7.2** | **Durante el empleo** | | | |
| **A.7.2.1** | Responsabilidades de la dirección | Aplica | Se debe socializar la política de seguridad de la información | Llevar el registro del cumplimiento de la política de seguridad de información |
| **A.7.2.2** | Adquisición de conciencia, educación y formación en la seguridad de la información | Aplica | No hay control centralizado pero si socialización de la política | Implementar un registro centralizado de la socialización de la política |
| **A.9.** | **Seguridad relativa a los Recursos Humanos** | | | |

| DECLARACION DE APLICABILIDAD | | | | |
|---|---|---|---|---|
| **Sección** | **Dominio, Objetivo de Control y controles** | **Aplicabilidad** | **Justificación** | **Recomendación** |
| **A.9.2** | **Gestión de Acceso de usuarios** | | | |
| **A.9.2.3.** | Gestión de derechos de acceso privilegiado | Aplica | No existen procedimientos | Se debe elaborar Procedimiento de gestión de asignación de privilegios |
| **A.9.3** | **Responsabilidades de Usuario** | | | |
| **A.9.3.1** | Uso de información de autenticación secreta | Aplica | Falta de Procedimiento de gestión de acceso a la información | Se debe elaborar procedimiento de gestión de acceso a la información |
| **A.9.4** | **Control de Acceso a Sistemas y Aplicaciones** | | | |

| DECLARACION DE APLICABILIDAD | | | | |
|---|---|---|---|---|
| **Sección** | **Dominio, Objetivo de Control y controles** | **Aplicabilidad** | **Justificación** | **Recomendación** |
| **A.9.4.3** | Sistema de gestión de contraseñas | Aplica | No existen mecanismos implementados para realizar la gestión de las contraseñas | Se debe implementar mecanismos para realizar la gestión de las contraseñas |
| **A.11.** | **Seguridad Física y del Entorno** | | | |
| **A.11.1** | **Áreas Seguras** | | | |
| **A.11.1.1** | Perímetro de seguridad | Aplica | Existen mecanismos de seguridad y control físico para proteger áreas que involucren información confidencial | |

| DECLARACION DE APLICABILIDAD | | | | |
|---|---|---|---|---|
| **Sección** | **Dominio, Objetivo de Control y controles** | **Aplicabilidad** | **Justificación** | **Recomendación** |
| **A.11.1.3** | Seguridad de oficinas, recintos e instalaciones | Aplica | Hay implementados controles para protección de las oficinas | |
| **A.11.1.4** | Protección contra amenazas externas y ambientales | Aplica | Se han implementado controles para protección contra desastres naturales externas o accidentes | |
| **A.11.2** | **Seguridad de los equipos** | | | |

| DECLARACION DE APLICABILIDAD | | | | |
|---|---|---|---|---|
| **Sección** | **Dominio, Objetivo de Control y controles** | **Aplicabilidad** | **Justificación** | **Recomendación** |
| **A.11.2.2** | Servicios de suministro | Aplica | Existe suministro de energía a través de UPS, no existe generador redundante | Se debe realizar la instalación de un generador |
| **A.11.2.4** | Mantenimiento de equipos | Aplica | Se realiza mantenimientos periódicos con personal calificado y autorizado | Llevar un control centralizado de las bitácoras de los mantenimientos |
| **A.12.** | **Seguridad de las operaciones** | | | |
| **A.12.1** | **Procedimientos y responsabilidades operacionales** | | | |

| DECLARACION DE APLICABILIDAD | | | | |
|---|---|---|---|---|
| **Sección** | **Dominio, Objetivo de Control y controles** | **Aplicabilidad** | **Justificación** | **Recomendación** |
| **A.12.1.2** | Gestión de cambio | Aplica | No se posee documentación de gestión de cambios de los sistemas | Elaborar documentación sobre gestión de cambio de los sistemas |
| **A.12.1.3** | Gestión de capacidad | Aplica | No se posee documentación sobre análisis y diagnósticos de la capacidad | Elaborar documentación sobre el control del desempeño y capacidad de los sistemas |
| **A.12.1.4** | Separación de los ambientes de desarrollo, pruebas, y operación | Aplica | Se realizan los ambientes de desarrollo y prueba en los equipos de los desarrolladores | Implementar ambientes de desarrollo y pruebas |

| DECLARACION DE APLICABILIDAD | | | | |
|---|---|---|---|---|
| **Sección** | **Dominio, Objetivo de Control y controles** | **Aplicabilidad** | **Justificación** | **Recomendación** |
| **A.12.2** | **Protección contra el software malicioso** | | | |
| **A.12.2.1** | Controles contra códigos maliciosos | Aplica | No existe control contra el código malicioso | Implementar controles contra código malicioso |
| **A.12.3** | **Copias de Seguridad** | | | |
| **A.12.3.1** | Respaldo de información | Aplica | No se tiene control para la verificación de respaldos | Implementar solución que permita verificar los respaldos |
| **A.12.4** | **Registro y Supervisión** | | | |
| **A.12.4.2** | Protección de la información | Aplica | No se cuenta con procedimientos para la | Implementación de Procedimientos y la |

| DECLARACION DE APLICABILIDAD | | | | |
|---|---|---|---|---|
| **Sección** | **Dominio, Objetivo de Control y controles** | **Aplicabilidad** | **Justificación** | **Recomendación** |
| | | | protección de la información | socialización de los mismos |
| **A.12.5** | **Control del Software en utilización** | | | |
| **A.12.5.1** | Instalación de software en sistemas operativos | Aplica | Los procedimientos están a cargo de la Dirección solamente | Socializar los procedimientos |
| **A.12.6** | **Gestión de la Vulnerabilidad técnica** | | | |
| **A.12.6.1** | Gestión de las vulnerabilidades técnicas | Aplica | Sólo se ha utilizado herramientas open para monitoreo de vulnerabilidades | Modernización de las herramientas de seguridad de la información |

| DECLARACION DE APLICABILIDAD | | | | |
|---|---|---|---|---|
| **Sección** | **Dominio, Objetivo de Control y controles** | **Aplicabilidad** | **Justificación** | **Recomendación** |
| **A.13** | **Seguridad de las Comunicaciones** | | | |
| **A.13.1** | **Gestión de la Seguridad de Redes** | | | |
| **A.13.1.2** | Seguridad de los Servicios de Red | Aplica | Los equipos de red se encuentran obsoletos, ya que no se han implementado mecanismos de seguridad | Modernización de los equipos/herramientas de redes y seguridad de la información |
| **A.13.2** | **Intercambio de la información** | | | |
| **A.13.2.1** | Políticas y procedimientos de | Aplica | No se cuenta con mecanismos de | Modernización de equipos de redes e |

| DECLARACION DE APLICABILIDAD | | | | |
|---|---|---|---|---|
| **Sección** | **Dominio, Objetivo de Control y controles** | **Aplicabilidad** | **Justificación** | **Recomendación** |
| | transferencia de información | | seguridad para la transferencia de información | implementar procedimientos de transferencia de información y socializarlos |
| **A.14** | **Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información** | | | |
| **A.14.1** | **Requisitos de Seguridad en los Sistemas de Información** | | | |
| **A.14.1.2** | Seguridad de Servicios de las aplicaciones en redes públicas | Aplica | No se cuenta con mecanismos para proteger la información | Implementar mecanismos para la protección de la información junto a la |

| DECLARACION DE APLICABILIDAD | | | | |
|---|---|---|---|---|
| **Sección** | **Dominio, Objetivo de Control y controles** | **Aplicabilidad** | **Justificación** | **Recomendación** |
| | | | ante posibles fuga de la misma | modernización de la infraestructura |
| **A.14.2** | **Seguridad en el Desarrollo y en el proceso de Soporte** | | | |
| **A.14.2.1** | Política de desarrollo seguro | Aplica | No se encuentran mecanismos de seguridad para protección de información en cuanto al desarrollo por parte del equipo | Se debe implementar los mecanismos de seguridad de la información como lo son los cifrados, las claves, etc. |

| DECLARACION DE APLICABILIDAD | | | | |
|---|---|---|---|---|
| **Sección** | **Dominio, Objetivo de Control y controles** | **Aplicabilidad** | **Justificación** | **Recomendación** |
| **A.14.2.2** | Procedimientos de control de cambios en sistemas | Aplica | No se cuenta con procedimientos de control de cambios dentro del ciclo de vida del desarrollo | Se debe realizar procedimientos de control de cambios aplicados al ciclo de vida del desarrollo |
| **A.14.2.9** | Prueba de aceptación de sistemas | Aplica | Las pruebas de aceptación no se realizan en base a un procedimiento operativo | Implementar Procedimientos para la realización de Pruebas de aceptación |
| **A.15** | **Relación con Proveedores** | | | |
| **A.15.1** | **Seguridad en las relaciones con proveedores** | | | |

| DECLARACION DE APLICABILIDAD | | | | |
|---|---|---|---|---|
| **Sección** | **Dominio, Objetivo de Control y controles** | **Aplicabilidad** | **Justificación** | **Recomendación** |
| **A.15.1.1** | Política de Seguridad de la información para las relaciones con proveedores | Aplica | No se cuenta con controles de seguridad para las relaciones con proveedores | Implementar los controles de seguridad para los servicios con proveedores |
| **A.15.2** | **Administración de aprovisionamiento de servicios de proveedores** | | | |
| **A.15.2.1** | Seguimiento y revisión de los servicios de los proveedores | Aplica | Implementar mecanismos para el seguimiento y revisión de los servicios de los proveedores | Crear registros del monitoreo de los servicios de los proveedores de forma centralizada |
| **A.16** | **Administración de Sucesos de Seguridad de la Información** | | | |

| DECLARACION DE APLICABILIDAD | | | | |
|---|---|---|---|---|
| **Sección** | **Dominio, Objetivo de Control y controles** | **Aplicabilidad** | **Justificación** | **Recomendación** |
| **A.16.1** | **Administración de Sucesos de Seguridad de la Información y Progresos** | | | |
| **A.16.1.1** | Responsabilidades y Procedimientos | Aplica | No se cuenta con procedimiento para la gestión de incidentes | Crear procedimiento para la gestión y recuperación ante incidentes |
| **A.16.1.3** | Reporte de debilidades de Seguridad de la Información | Aplica | No se obtienen reportes de incidentes por parte del personal | Crear procedimiento para concientizar sobre los incidentes de Seguridad de la Información |

| DECLARACION DE APLICABILIDAD | | | | |
|---|---|---|---|---|
| **Sección** | **Dominio, Objetivo de Control y controles** | **Aplicabilidad** | **Justificación** | **Recomendación** |
| **A.16.1.4** | Valoración de sucesos de la Seguridad de la Información y resolución sobre ellos | Aplica | No se cuenta con procedimiento para la gestión de incidentes | Desarrollar procedimiento para la gestión de incidentes que evalúe la seguridad de la información de manera integral |
| **A.16.1.5** | Respuesta a Incidentes de Seguridad de la Información | Aplica | Plan de Continuidad del Negocio se encuentra Obsoleto | Actualizar procedimiento para el manejo de incidentes y vulnerabilidades de la seguridad de la información |

| DECLARACION DE APLICABILIDAD | | | | |
|---|---|---|---|---|
| **Sección** | **Dominio, Objetivo de Control y controles** | **Aplicabilidad** | **Justificación** | **Recomendación** |
| **A.17** | **Figura de la Seguridad de la Información para la Administración de la Continuidad del Negocio** | | | |
| **A.17.1** | **Estabilidad para la Seguridad de la Información** | | | |
| **A.17.1.2** | Implementación de continuidad de la Seguridad de la Información | Aplica | Implementar redundancia para el servicio cloud, energía eléctrica en las oficinas donde opera la empresa | Se debe implementar proveedor externo de servicio cloud y adquirir e instalar un generador para suministro alterno de energía eléctrica |
| **A.17.2** | **Redundancias** | | | |
| **A.17.2.1** | Disponibilidad de Instalaciones de | Aplica | Al momento no se cuenta con un sitio | Implementar Plan de Sitio alterno para la |

| DECLARACION DE APLICABILIDAD | | | | |
|---|---|---|---|---|
| **Sección** | **Dominio, Objetivo de Control y controles** | **Aplicabilidad** | **Justificación** | **Recomendación** |
| | procesamiento de información | | alterno para la continuidad del negocio | continuidad de las operaciones |
| **A.18** | **Cumplimiento** | | | |
| **A.18.2** | **Revisiones de la Seguridad de la Información** | | | |
| **A.18.2.3** | Revisión del cumplimiento técnico | Aplica | No se cuenta con procedimiento para la revisión del cumplimiento técnico | Elaborar procedimiento que permita la revisión del cumplimiento técnico |