ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

CENTRO DE EDUCACIÓN CONTINUA

DIPLOMADO SUPERIOR EN AUDITORIA INFORMÁTICA

III PROMOCIÓN

PROYECTO

TEMA

"Establecer un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001"

AUTORES:

Ing. Rodrigo Fernando Morocho Román

Ing. Wilmer Braulio Rivas Asanza

AÑO

2010

Tabla de contenido

1. OBJETIVO

Establecer un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001 para la empresa Orotoni Cía. Ltda., que le permita garantizar razonablemente la Integridad, Confidencialidad y Disponibilidad de la Información.

2. INTRODUCCIÓN

Hoy en día una gran cantidad de organizaciones sean públicas o privadas, de tamaño micro, medianas o multinacionales, están amenazadas continuamente en sus activos por riesgos que ponen en peligro la integridad, confidencialidad y disponibilidad de la información, lo mismo que la consecución de los objetivos del negocio, riesgos que provienen tanto del exterior como del interior de las organizaciones, los puntos débiles de los sistemas de información pueden representar graves problemas, de tal forma que para poder trabajar en un entorno como este de manera segura, las empresas pueden asegurar sus datos e información de valor con la ayuda de un Sistema de Gestión de Seguridad de la Información (SGSI).

La Seguridad de la Información se refiere a la protección de los activos de información fundamentales para el éxito de las organizaciones, esta seguridad puede ser establecida con ayuda de la norma ISO/IEC 27001, al implementar un modelo de administración de la seguridad de la información basada en las mejores prácticas existentes en el mercado, como la norma ISO/IEC 27001, las organizaciones protegen su información contra las amenazas y vulnerabilidades, asegurando con esto la continuidad de sus negocios y minimizando los riesgos a los que están expuestas.

En las organizaciones del medio el tema de certificación en aspectos de seguridad de la información, aún no ha sido considerado con la seriedad que merece, sin embargo, no cabe duda que lo será en poco tiempo. Se puede decir, que la certificación ISO/IEC 27001, será casi una obligación de cualquier empresa que desee competir en el mercado en el corto plazo, lo cual es lógico, pues si se desea interrelacionar sistemas de clientes, control de stock, facturación, pedidos, productos, etc. entre diferentes organizaciones, se deben exigir mutuamente niveles concretos y adecuados de seguridad de la información.

3. DESCRIPCIÓN GENERAL DE LA EMPRESA

3.1 Datos Informativos

3.1.1 Reseña Histórica

Desde hace 22 años la Sra. Enma Abril, comercializa los productos de INDUSTRIAS LACTEAS TONI S.A. basados en el trabajo, con la mística en el servicio al cliente logrando en los actuales momentos tener un sitial importante en el mercado de la Provincia de El Oro. Teniendo actualmente 3.860 clientes activos de los cuales el 70% son de línea de cobertura (minoristas) con un volumen de drop size de $ 7,00 con una emisión de 650 facturas.

En el año 2002, se toma la decisión de constituirse como compañía y nace "OROTONI CÍA. LTDA.", continuando con los mismos objetivos de convertirse en líderes de la distribución y comercialización de líneas de productos de alta calidad, incrementar nuestros clientes (especialmente de cobertura), para alcanzar la rentabilidad que garantice el bienestar de todos quienes conforman OROTONI CÍA. LTDA.

En el mes de noviembre del año 2005 se da apertura al RUC 0702846619001 a nombre del Sr. Oswaldo Apolo por motivo de pérdida del crédito tributario en declaraciones de IVA, ya que se comercializaba productos de tarifa 0% y 12%.

La fuerza de ventas opera en toda la provincia de El Oro, vía a la provincia del Guayas (Balao, La Ponce, Tenguel), y parte de la provincia de Loja (Macará, Alamor, Zapotillo, Celica, La Toma).

3.1.2 Misión

La Empresa Orotoni Cía. Ltda., tiene como misión propia "distribuir distintas líneas de productos y muy particularmente productos Toni, aplicando procedimientos con el objetivo de tener una amplia cantidad de clientes bien atendidos".

3.1.3 Visión

La Empresa Orotoni Cía. Ltda., tiene como visión cubrir todos los clientes de las Provincias de: El Oro, Loja y parte del Guayas, ofreciéndole la distribución de diversas líneas de productos y muy en particular la línea TONI.

3.1.4 Organigrama

Ver Anexo A1.

3.2 Datos Operativos

RECURSOS MATERIALES

Terreno (todo con cubierta de estructura metálica)	2.000 m^2
Área de bodegas	1.000 m^2
Área de garaje-carga-descarga-despacho	600 m^2
Área oficinas administrativas	400 m^2
Camiones para el reparto	12
Camioneta de apoyo	1
Cámaras de frío	3

MARCAS DE PRODUCTOS EN DISTRIBUCION

MARCAS	PRODUCTOS
TONI	• Yogurt • Gelatoni • Cereales
TOPSY	• Helados en peletería • Tortas • Tachos
TAMPICO	• Tampico Pet • Tampico Light
WINTER	• Gomas de Mascar
CRISSAL	• Sal Yodada

ZAIMELLA	• Línea Cosmética Infantil • Pañales Desechables

3.3 Datos Tecnológicos

3.3.1 Hardware

Servidor de Aplicaciones:

- **Procesador**

  AMD® Sempron™ LE 1300; 2.3GHz, 512K Caché

- **Memoria**

  DDR2 de 1GB, 800MHz, 1x1G, Dual Ranked DIMM

- **Disco Duro**

  SATA 160GB 7.2K RPM 3Gbps 3.5-in Cabled

Equipos de usuario:

COMPUTADORAS PENTIUM 4 3.0 GHZ

- Mainboard INTEL 915 D101 V/S/R LGA
- Procesador Intel 3.0 Ghz PENTIUM 4 REAL
- Disco Duro 80 Gb 7200 RPM
- Memoria 512 MB DDR400
- Quemador de DVD 16x LG DVDRW-DVDROM + CDRW + CDROM
- Video 256 MB Integrado ATi Xpress 2000
- Sonido 3D Integrado
- Red 10/100 Integrado
- Floppy 1.44 MB
- Teclado Multimedia Ps/2
- Mouse Optico Scroll Ps/2
- Parlantes Externos 300W
- Case P4 ATX 450/500w USB
- Monitor 17' LG FLATRON

3.3.2 Aplicaciones

Hace 8 años la Fábrica de Productos Toni, negoció un sistema denominado Power Street, cuyos desarrolladores son del Uruguay, este producto fue negociado también para las distribuidoras entre ellas Orotoni Cía. Ltda., la empresa desarrolladora es Assist Ltda., es una empresa con 16 años de experiencia, cuenta con una cartera de más de 450 empresas en toda Latinoamérica.

Power Street facilita la gestión con procesos y operaciones eficientes, reduce los costos operativos, aumenta la participación en el mercado mediante la aplicación de políticas de ventas dinámicas, flexibles y agresivas, dejando sin capacidad de respuesta a la competencia, controla la operación independiente del esquema de distribución y del modelo de negocio.

Logo de Aplicación Power Street

Power Street una solución 100% Uruguaya, www.assist.com.uy, hoy es líder en su segmento a nivel de Latinoamérica con presencia en 17 países, ha permitido optimizar los procesos, ser más eficientes en la utilización de los recursos, utilizar las mejores prácticas de gestión del cliente aplicadas por la grandes compañías a nivel mundial como Philip Morris - Unilever - Danone - Ambev - Clrorox etc., permite implementar mejoras sustanciales en la calidad, la atención, el servicio y apoyo a los clientes.

Características de la aplicación

3.4 Problemática de la situación actual respecto de la Seguridad de la Información

La problemática de la seguridad en los sistemas de información surge del desarrollo e implantación de tecnologías de información y comunicación. La rápida implantación que ha tenido Internet en nuestras vidas ha conllevado que cantidades enormes de información (en muchos casos confidencial) estén a disposición de cualquiera. Esta escasa seguridad que hubo en los orígenes del boom de Internet hizo saltar la alarma, de tal forma que la seguridad de la información empezó a tomarse en serio, tanto en el ámbito empresarial, como comercial y por supuesto jurídico-legal.

Pero esta seguridad no afecta sólo al tráfico que circula por la red. Debe entenderse la seguridad como algo integral. Debe abordar problemas desde tráfico en red, hasta seguridad física de servidores y bases de datos de información.

Los gerentes de seguridad de la información han esperado mucho tiempo a que alguien tomara el liderazgo para producir un conjunto de normas de seguridad de la información que estuviera sujeto a auditoría y fuera reconocido globalmente. Se cree que un código de normas de la seguridad apoyaría los esfuerzos de los gerentes de tecnología de la información en el sentido que facilitaría la toma de decisión de compra, incrementaría la cooperación entre los múltiples departamentos por ser la seguridad el interés común y ayudaría a consolidar la seguridad como prioridad empresarial.

ISO 27001 surge como la norma técnica de seguridad de la información reconocida a nivel mundial. ISO 27001 se define como "un completo conjunto de controles que incluye las prácticas exitosas de seguridad de la información".

La problemática aquí expuesta es soportada por varios estudios e informes, como los publicados por tres importantes consultoras internacionales como:

Pricewaterhousecoopers, Ernst & Young y Deloitte, sobre los estados globales de la seguridad de la información, como el extracto publicado en el sitio www.segu-info.ar al cuál se hace referencia a continuación:

Por un lado PricewaterhouseCoopers entrevistó alrededor de 7000 ejecutivos extrayendo los siguientes datos:

- Los niveles de seguridad implementados siguen siendo reactivos, necesitando justamente que los procesos implementados deban ser proactivos y que permitan la prevención de problemas, vulnerabilidades y desastres.
- No se dedican esfuerzos y fondos necesarios para implementar medidas de seguridad, siendo marketing y recursos humanos las áreas a las que se destina mayor cantidad de recursos.

- Se sigue invirtiendo en mayor cantidad de recursos tecnológicos como: cifrado, backup, sistemas de detección de intrusos, firewall, etc., sin considerar como parte del proceso al personal, la estrategia y la gestión, siendo estos los principales problemas que se enfrentaron con casos millonarios de fuga de información en las empresas.

- Los medios utilizados para los delincuentes siguen siendo los triviales, muy conocidos pero altamente efectivos en personal sin concientización (ingeniería social, phishing, malware, robo de laptops, etc.)

- Las regulaciones y políticas internaciones –como Sarbanes-Oxley (SOX)- empujan a las empresas hacia la gestión de la seguridad de la información.

- Uno de los puntos más preocupantes es aquel que menciona que pocas organizaciones tienen una conciencia sobre las empresas externas que utilizan sus datos y muchas de ellas ni siquiera conoce o le exige cumplir las políticas de privacidad a esas otras empresas. El principal motivo que se exhibe en este caso es el costo asociado a verificar esta información.

- Sólo 2 de 10 empresas consideran la clasificación de la información como parte del proceso en la implementación de políticas de seguridad.

- Sigue siendo difícil determinar la forma en que se produjo una brecha de seguridad. En este aspecto, la ignorancia es el principal factor a mitigar.

Ernst & Young entrevistó alrededor de 1400 profesionales de seguridad, extrayendo la siguiente información:

- Se ha vuelto fundamental proteger la reputación y la marca de la empresa, ya que las mismas son difíciles de construir y muy fácil de dañar con un sólo hecho desafortunado.

- Los estándares internacionales y las buenas prácticas, como ISO 27001:2005, siguen ganado gran aceptación en el mercado.

- Existe una gran brecha entre la necesidad de la privacidad y las medidas que se toman para mitigar los riesgos asociados.

- Las organizaciones no están dispuestas a realizar los procesos de gestión de seguridad de la información a través del outsourcing, manteniendo estas actividades en áreas internas de la empresa, relacionando esta decisión al compromiso de proteger la reputación.

- Pocas compañías aceptan asegurar sus recursos contra ciberataques y este tipo de seguro no ha logrado expandirse a pesar de que hace tiempo de que es ofrecido por las empresas de seguros. Esta podría ser una forma de cubrir muchos de los riegos desconocidos mencionados anteriormente.

Finalmente, Deloitte, publicó su informe que refleja el estado en seguridad de las 250 principales compañías financieras de 32 países de todo el mundo:

- Muchas organizaciones buscan comprometerse con las buenas prácticas internacionales en seguridad, siendo la pérdida de información un punto que comienza a tenerse en cuenta.

- Se nota un incremento importante en la adopción de la figura de CISO (Chief Information Security Officer) como una figura relacionada a la gestión de la seguridad.

- Se comienza a notar una mayor preocupación de las organizaciones para prevenir o bloquear amenazas internas.

- Nuevamente se destaca la importancia de las regulaciones, los procesos definidos y documentados.

- La administración de identidad sigue siendo un factor preocupante debido a la alta cantidad de usuarios móviles.

- Los CISO tienen a cargo áreas diferentes de IT y siguen sin incluirse tareas como administración de identidad, perímetros de seguridad, móviles, gestión de políticas, etc.

- La mayoría opina que la seguridad física no converge con la seguridad lógica.

- El mayor impedimento para implementar medidas de seguridad sigue siendo el presupuesto.

- Los proyectos de seguridad muchas veces fallan porque aparecen mayores desafíos o prioridades dentro de la compañía.

- No existen proyectos que verifiquen la seguridad en el ciclo de vida del software.

- La mayoría de los errores son humanos, de tecnología y de procesos.

- No se conducen estudios de seguridad dentro de las compañías.

Extrapolando los 3 estudios, se pueden extraer algunas conclusiones, que se resumen a continuación:

- Es necesario invertir más concientización y educación en seguridad.

- Se debe comenzar a considerar a los recursos humanos por encima de los tecnológicos.

- Se debe empezar a considerar la moral y la ética en los procesos de las compañías.

- Las regulaciones, los estándares y las buenas prácticas se han transformado en un gran aliado y ayuda en la gestión.

- La reputación es un activo de gran valor que se debe proteger.

- Se conocen muchos de los riesgos pero se ignoran o aún no se toman las contramedidas necesarias para mitigarlos (incluso los seguros).

- En seguridad todavía no se establecen estrategias que involucren a las áreas gerenciales, como sí sucede en otros sectores de las compañías. El porcentaje de CISOs que reportan a un comité de seguridad es extremadamente bajo, reportando la mayoría de ellos al CIO de la compañía.

- La información confidencial, privada y personal todavía no cuenta con las medidas de protección adecuadas.

- Los insiders (atacantes internos) son una preocupación cada vez mayor y las compañías deben trabajar más en este aspecto.

- La seguridad física sigue siendo vista como un proceso aislado del resto de la gestión de seguridad.

- Se sigue confundiendo las funciones y se sigue invirtiendo en IT.

- El SDLC (Software Development LifeCycle) sigue sin considerar la seguridad.

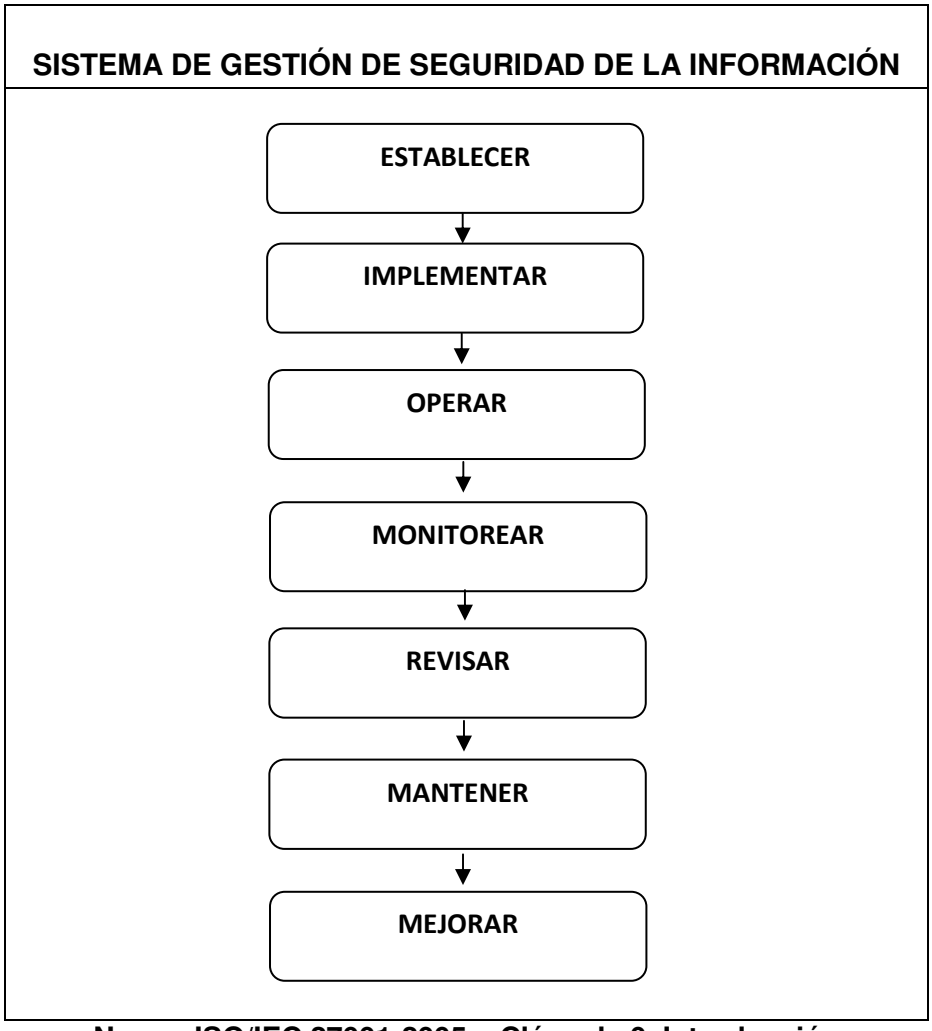
- Lamentablemente, muchos proyectos de seguridad no se alinean o se alinean poco con los objetivos de la compañía, lo que hace que el proyecto termine fracasando.

- Es necesario un presupuesto disponible para la adecuada gestión de la seguridad.

4. PROPUESTA METODOLÓGICA PARA EL DESARROLLO Y MANTENIMIENTO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN LA NORMA ISO/IEC 27001:2005

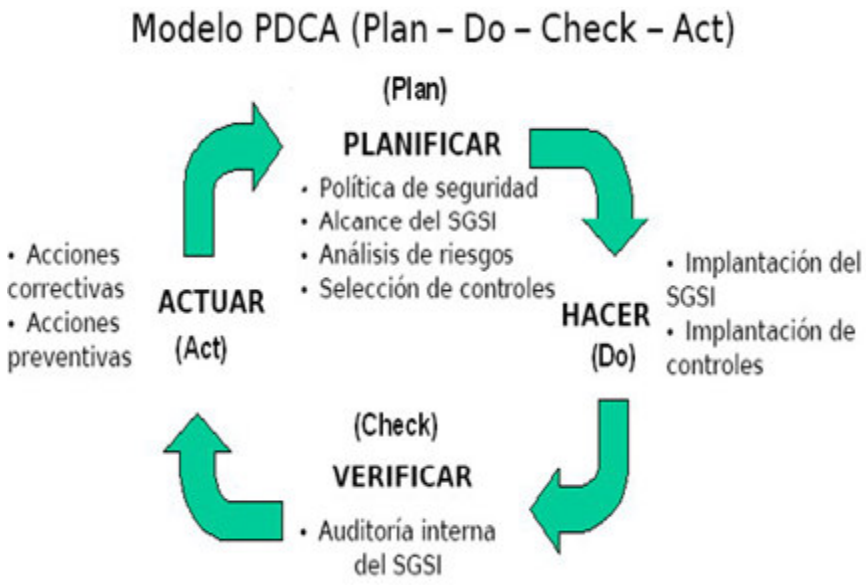
La norma ISO 27001 es una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización.

La norma ISO 27001 define la información como un activo que posee valor para la organización y requiere por tanto de una protección adecuada. El objetivo de la seguridad de la información es proteger adecuadamente este activo para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio.



Norma ISO/IEC 27001:2005 – Cláusula 0. Introducción

Para el desarrollo y mantenimiento del SGSI se adopta la metodología PDCA:



Norma ISO/IEC 27001:2005 – Cláusula 0. Introducción

Plan: Establecer el SGSI

- Definir el alcance del SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión.

- Definir una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos del negocio, además de establecer los criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable. Lo primordial de esta metodología es que los resultados obtenidos sean comparables y repetibles (existen numerosas metodologías estandarizadas para la evaluación de riesgos, aunque es perfectamente aceptable definir una propia).
- Identificar los riesgos:
    - identificar los activos que están dentro del alcance del SGSI y a sus responsables directos, denominados propietarios;
    - identificar las amenazas en relación a los activos;

  - identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas;
  - identificar los impactos en la confidencialidad, integridad y disponibilidad de los activos.

- Analizar y evaluar los riesgos:

  - evaluar el impacto en el negocio de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información;
  - evaluar de forma realista la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados;
  - estimar los niveles de riesgo;
  - determinar, según los criterios de aceptación de riesgo previamente establecidos, si el riesgo es aceptable o necesita ser tratado.

- Identificar y evaluar las distintas opciones de tratamiento de los riesgos para:

  - aplicar controles adecuados;
  - aceptar el riesgo, siempre y cuando se siga cumpliendo con las políticas y criterios establecidos para la aceptación de los riesgos;
  - evitar el riesgo, p. ej., mediante el cese de las actividades que lo originan;
  - transferir el riesgo a terceros, p. ej., compañías aseguradoras o proveedores de outsourcing.

- Seleccionar los objetivos de control y los controles del Anexo A de ISO 27001 para el tratamiento del riesgo que cumplan con los requerimientos identificados en el proceso de evaluación del riesgo.
- Aprobar por parte de la dirección tanto los riesgos residuales como la implantación y uso del SGSI.
- Definir una declaración de aplicabilidad que incluya:

  - los objetivos de control y controles seleccionados y los motivos para su elección;

- los objetivos de control y controles que actualmente ya están implantados;

En relación a los controles de seguridad, el estándar ISO 27002 (antigua ISO 17799) proporciona una completa guía de implantación que contiene 133 controles, según 39 objetivos de control agrupados en 11 dominios. Esta norma es referenciada en ISO 27001, en su segunda cláusula, en términos de "documento indispensable para la aplicación de este documento" y deja abierta la posibilidad de incluir controles adicionales en el caso de que la guía no contemplase todas las necesidades particulares.

Do: Implementar y utilizar el SGSI

- Definir un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.
- Implantar el plan de tratamiento de riesgos, con el fin de alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades.
- Implementar los controles anteriormente seleccionados que lleven a los objetivos de control.
- Definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles.
- Procurar programas de formación y concienciación en relación a la seguridad de la información a todo el personal.
- Gestionar las operaciones del SGSI.
- Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información.
- Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.

Check: Monitorizar y revisar el SGSI

La organización deberá:

- Ejecutar procedimientos de monitorización y revisión para:

  - detectar a tiempo los errores en los resultados generados por el procesamiento de la información;
  - identificar brechas e incidentes de seguridad;
  - ayudar a la dirección a determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad de la información se desarrollan en relación a lo previsto;
  - detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores;
  - determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas.
  - Revisar regularmente la efectividad del SGSI, atendiendo al cumplimiento de la política y objetivos del SGSI, los resultados de auditorías de seguridad, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas.

- Medir la efectividad de los controles para verificar que se cumple con los requisitos de seguridad.
- Revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que hayan podido producirse en la organización, la tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles implementados y el entorno exterior -requerimientos legales, obligaciones contractuales, etc.
- Realizar periódicamente auditorías internas del SGSI en intervalos planificados.
- Revisar el SGSI por parte de la dirección periódicamente para garantizar que el alcance definido sigue siendo el adecuado y que las mejoras en el proceso del SGSI son evidentes.
- Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.
- Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI.

Act: Mantener y mejorar el SGSI

La organización deberá regularmente:

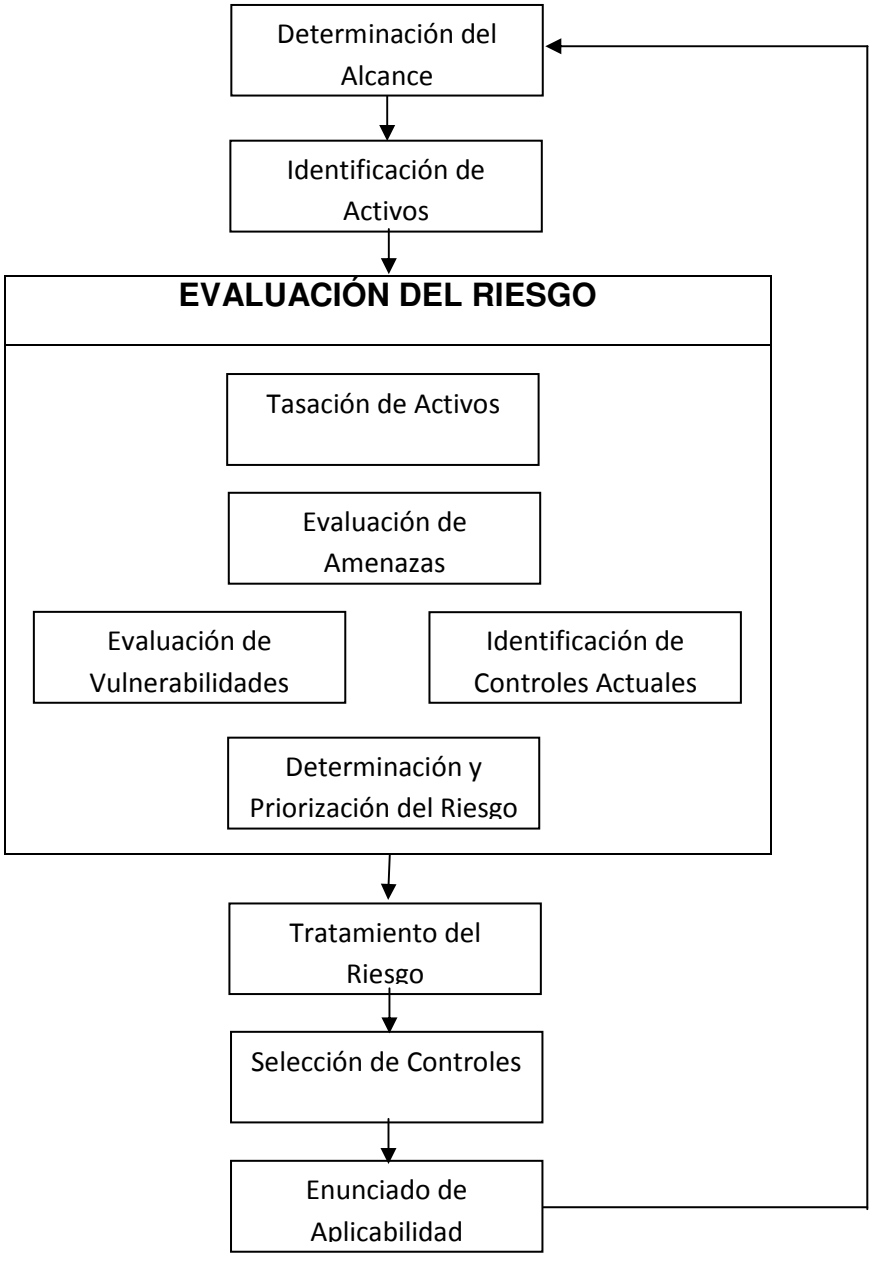
- Implantar en el SGSI las mejoras identificadas.
- Realizar las acciones preventivas y correctivas adecuadas en relación a la cláusula 8 de ISO 27001 y a las lecciones aprendidas de las experiencias propias y de otras organizaciones.
- Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.
- Asegurarse que las mejoras introducidas alcanzan los objetivos previstos.

PDCA es un ciclo de vida continuo, lo cual quiere decir que la fase de Act lleva de nuevo a la fase de Plan para iniciar un nuevo ciclo de las cuatro fases. Téngase en cuenta que no tiene que haber una secuencia estricta de las fases, sino que, p. ej., puede haber actividades de implantación que ya se lleven a cabo cuando otras de planificación aún no han finalizado; o que se monitoricen controles que aún no están implantados en su totalidad.

La norma se desarrolla en 11 áreas o dominios que recogen los 133 controles a seguir, los dominios son:

- Política de seguridad
- Organización de la información de seguridad
- Administración de recursos
- Seguridad de los recursos humanos
- Seguridad física y del entorno
- Administración de las comunicaciones y operaciones
- Control de accesos
- Adquisición de sistemas de información, desarrollo y mantenimiento
- Administración de los incidentes de seguridad
- Administración de la continuidad de negocio
- Marco legal y buenas prácticas

5. PROPUESTA METODOLÓGICA PARA EL ESTABLECIMIENTO DEL SGSI PARA OROTONI CÍA. LTDA. SEGÚN LA NORMA ISO/IEC 27001:2005



Metodología para el Establecimiento del SGSI según la norma ISO/IEC 27001:2005

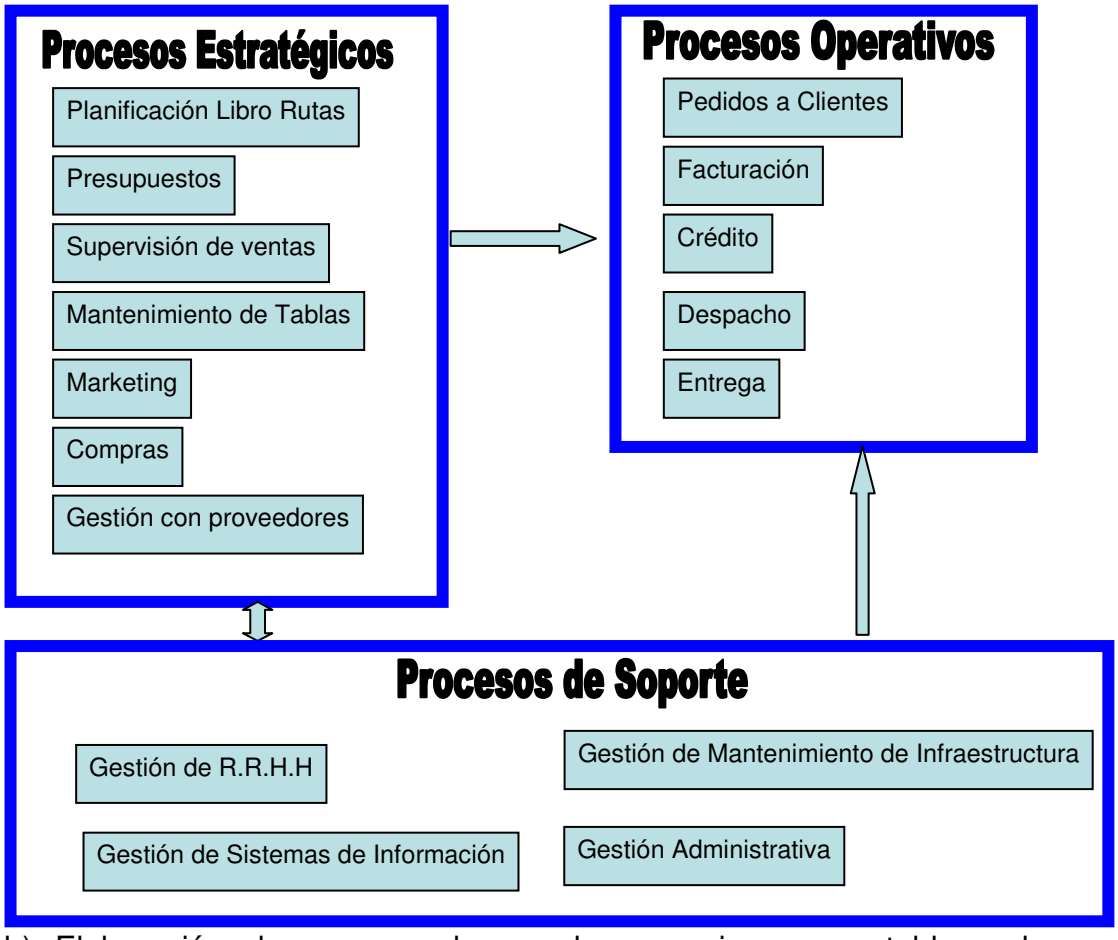
5.1 Determinación del Alcance

El presente proyecto pretende establecer un Sistema de Gestión de Seguridad de la Información para la empresa OROTONI Cía. Ltda., cuyo alcance abarque los procesos y actividades principales de la empresa, estos procesos y actividades se han seleccionado en base a las preocupaciones presentadas por la gerencia, se busca de esta manera que la gestión de la seguridad esté alineada con los objetivos del negocio y así proteger aquello que para la organización es el punto central de sus actividades.

Para determinar el alcance se aplicará los siguientes conceptos:

a) Elaboración del Mapa de Procesos de la institución que especifique los procesos estratégicos, operativos y de soporte.

Mapa de Procesos de OROTONI Cía. Ltda.:



b) Elaboración de un acuerdo con la gerencia para establecer los procesos a partir de los cuales se realizará la evaluación de riesgos para identificar los objetivos de control.

Acuerdo:

1) La Empresa Orotoni Cía. Ltda., declara a través del presente acuerdo, que los procesos que serán considerados para el establecimiento del SGSI, dada su criticidad para la organización, son los siguientes:

Proceso Estratégico	• Mantenimiento de Tablas
Procesos Operativos	• Pedidos a clientes • Facturación • Crédito

2) Localizaciones físicas incluidas

Detalle de los límites físicos del SGSI:

Ver Anexo A2.

3) Actividades de la Organización

Descripción de los procesos seleccionados

Proceso Estratégico

Mantenimiento de Tablas

Descripción: Se es responsable de crear un nuevo producto, vendedor, proveedor, políticas de venta, clientes, anular documentos, manipular los parámetros del sistema.

Por ser un distribuidor de la fábrica TONI en Guayaquil, vía sincronización de datos ellos actualizan datos con los productos que corresponden a la línea TONI.

Responsable	Sistemas, Sistemas Guayaquil
Revisado	
Actores	Clientes, vendedores, crédito, sistemas
Pre-condiciones	Existir necesidades de cambios
Acciones	Mantenimiento de cambios de parámetros del sistema
Post-condiciones	Cambios en Producción
Instrucciones de Trabajo	Verificar necesidad Verificar necesidad con autorización Proceder con el cambio

Procesos Operativos

Pedidos a Clientes

Descripción: A los vendedores se les asigna un libro de rutas (grupo de clientes que se les asigna a los vendedores para que los visite y recepte los pedidos diariamente). Este libro de rutas es elaborado por el jefe de ventas. Los vendedores recorren durante el día cubriendo la ruta, en la tarde cuando han terminado su ruta llegan a la empresa y entregan sus pedidos al facturador quien se encarga de digitar los pedidos en el sistema.

En la actualidad existen 12 vendedores de los cuales 5 tienen pockets, significa que 7 traen los pedidos en papel.

Responsable	Vendedor – Facturador
Revisado	
Actores	Vendedores, Facturador, Clientes
Pre-condiciones	Registrar libro de rutas Conocimiento de la ruta Conocimiento de los productos. Conocimiento del sistema
Acciones	Realizar el pedido
Post-condiciones	Registrar en el sistema el pedido Generar factura
Instrucciones de Trabajo	Realizar durante el día Entregar en la empresa los pedidos(en papel o en pockets) Si lo hacen a mano codificar los clientes correctamente. Si lo hacen a mano codificar los productos y cantidades correctamente

Facturación

Descripción: Facturación trabaja a partir de que los vendedores traen los pedidos, esto es aproximadamente a partir de las 4 de la tarde, emite las facturas que los vendedores traen en pockets, digita y emite de los vendedores que traen en papel. Asigna grupos de facturas a una liquidación que se agrupan de acuerdo al despacho y recorrido de entrega al día siguiente.

Toda la facturación se la emite con la fecha del día siguiente.

Todas las facturas son consideradas al contado excepto las autorizadas por Crédito cuyo control se lo hace automáticamente en el sistema.

Responsable	Facturador
Revisado	
Actores	Vendedores, Facturador, Clientes, Bodega
Pre-condiciones	Registrar el pedido Conocimiento de las rutas Conocimiento de los productos Conocimiento del sistema
Acciones	Generar la factura, liquidaciones, despachos
Post-condiciones	Generar los Despachos Generar las liquidaciones
Instrucciones de Trabajo	Realizar luego que traen los pedidos los vendedores Controlar que las facturas emitidas estén correctas Emitir las liquidaciones Emitir los Despachos

Crédito

Descripción: Existen muchos clientes que pagan con cheques posfechado, crédito se encarga de asignar a cada vendedor las facturas que son consideras como créditos.

Se encarga de hacer las cancelaciones producto del cuadro con la liquidación que traen los vendedores.

Responsable	Facturador, Agente de Crédito
Revisado	
Actores	Vendedores, Facturador, Clientes, Agente de crédito
Pre-condiciones	Registrar el pedido Conocimiento de los clientes Conocimiento de los productos Conocimiento del sistema
Acciones	Generar la cobranza, liquidaciones de pago
Post-condiciones	Generar los Despachos Generar las liquidaciones
Instrucciones de Trabajo	Realizar luego que traen los pedidos los vendedores Controlar que las facturas emitidas estén correctas Emitir las liquidaciones Emitir los Despachos

4) Quedan excluidos del alcance:

Procesos Estratégicos	• Planificación libro de rutas • Presupuestos • Supervisión de ventas • Marketing • Compras

	• Gestión con proveedores
Procesos Operativos	• Despacho • Entrega
Procesos de Soporte	• Gestión de RR.HH • Gestión de Mantenimiento de Infraestructura • Gestión Administrativa

Estos procesos han sido excluidos dado que hasta el momento la gerencia no los considera críticos para la consecución de sus objetivos, se anexa una carta (Anexo A3) en la cual la gerencia describe que los riesgos asociados a estos procesos han sido aceptados.

5.2 Identificación de Activos

Para cada proceso se identifican los activos involucrados.

Proceso: Mantenimiento de Tablas

Hardware	• Computador
Software de Información	• Sistema power street • Sistema Visual Fac
Información	• Libro de rutas • Vendedores • Clientes • Producto
Personas	• Vendedores • Clientes • Facturador

Proceso: Pedidos a Clientes

Hardware	• Pockets • Computador
Software de Información	• Sistema power street

Información	• Libro de rutas • Vendedores • Clientes
Personas	• Vendedores • Bodeguero • Facturador

Proceso: Facturación

Hardware	• Pockets • Computador
Software de Información	• Sistema power street
Información	• Libro de rutas • Vendedores • Clientes • Documento de factura
Personas	• Vendedores • Facturador • Bodeguero

Proceso: Crédito

Hardware	• Computador
Software de Información	• Sistema Power Street • Sistema Visual Fac
Información	• Libro de rutas • Vendedores • Clientes • Documento de factura • Documento de crédito
Personas	• Vendedores • Facturador • Agente de Crédito

5.3 Evaluación del Riesgo

Las metodologías de análisis de riesgos difieren esencialmente en la manera de estimar la probabilidad de ocurrencia de una amenaza y en la forma de determinar el impacto en la organización.

La metodología a utilizar es la cualitativa (Qualitative risk analysis), en la cual se usa una escala de puntuaciones para situar la gravedad del impacto, dando una caracterización de "alta/media/baja", la escala de puntuación queda establecida de la siguiente manera:

1 = Caracterización de Baja

2 = Caracterización de Media

3 = Caracterización de Alta

El valor del riesgo será resultado del promedio entre el valor del activo y la posibilidad de ocurrencia de amenaza y vulnerabilidad, una vez realizados los promedios, los resultados se ponderarán del modo siguiente:

La realización de un análisis de riesgos es un proceso laborioso, para cada activo se van a valorar todas las amenazas que pueden afectarle, la vulnerabilidad de cada una de las amenazas y el impacto que causaría la amenaza en caso de ocurrir. Con todos esos datos, se calcula el valor del riesgo para ese activo.

5.3.1 Tasación de activos

Para conocer la fuente de obtención de la calificación de los cuadros de Tasación de Activos y Priorización del Riesgo, ver Anexo A5.

Proceso: Mantenimiento de Tablas

Activos	Tasación			
	Confidencialidad	Integridad	Disponibilidad	Total
Computador	3	3	3	3
Vendedores	3	3	3	3
Clientes	3	3	3	3
Productos	3	3	3	3
Sistema Power Street	3	3	3	3

Sistema Visual Fac	3	3	3	3
Libro de rutas	3	3	2	2.67
Vendedor	3	3	3	3
Cliente	3	3	3	3
Productos	3	3	3	3

Proceso: Pedidos a Clientes

Activos	Tasación			
	Confidencialidad	Integridad	Disponibilidad	Total
Pockets	3	3	1	2.33
Computador	3	3	3	3
Vendedores	3	3	2	2.67
Facturador	3	2	2	2.33
Bodega	3	2	2	2.33
Sistema Power Street	3	3	3	3
Inf. Del cliente (informativo)	3	3	2	2.67
Inf. Del cliente (pedidos)	3	3	2	2.67
Inf. Del vendedor	3	3	2	2.67
Libro de rutas	3	2	2	2.33
Vendedor	3	3	2	2.67
Cliente	3	3	2	2.67

Proceso: Facturación

Activos	Tasación			
	Confidencialidad	Integridad	Disponibilidad	Total
Pockets	3	3	1	2.33
Computador	3	3	3	3
Vendedores	3	3	2	2.67
Facturador	3	3	3	3
Bodega	3	3	2	2.67
Sistema Power Street	3	3	3	3

Inf. Del cliente (informativo)	3	2	3	2.67
Inf. Del cliente (pedidos)	3	3	3	3
Inf. Del vendedor	3	2	2	2.33
Libro de rutas	3	2	2	2.33
Vendedor	3	3	2	2.67
Cliente	3	3	2	2.67
Factura	3	3	3	3

Proceso: Crédito

Activos	Tasación			
	Confidencialidad	Integridad	Disponibilidad	Total
Computador	3	3	3	3
Vendedores	3	3	2	2.67
Facturador	3	3	3	3
Crédito	3	3	3	3
Sistema Power Street	3	2	1	2
Sistema Visual Fac	3	3	3	3
Factura - Cancelaciones	3	3	3	3
Libro de rutas	3	2	2	2.33
Vendedor	3	3	2	2.67
Cliente	3	3	2	2.67
Factura	3	3	3	3
Crédito	3	3	3	3

5.3.2 Evaluación de Amenazas – Evaluación de Vulnerabilidades – Identificación de Controles Actuales – Determinación y Priorización del Riesgo

Proceso Mantenimiento de Tablas

Activos	Amenazas	Posibilidad Ocurrencia de la Amenaza	Vulnerabilidad	Posibilidad Que la amenaza Explote la vulnerabilidad	Valor Del Activo	Posible Ocurrencia de Amenaza y Vulnerabilidad	Total	Criticidad
computador	Fallo en el equipo	1	Falta de mantenimiento Falta de un buen entorno operativo	2 2	3	1.7	2.3	
	Falta de energía	2	Falta de un generador eléctrico Falta de un control operativo de los ups individuales.	2 2				
	Mal uso	1	Falta capacitación	2				
	Virus Informático	2	Políticas de seguridad No existe la adquisición de licencias de un antivirus	2 2				
Vendedores	Falta de Responsabilidad	2	Políticas para seleccionar personal Falta de incentivos y atención a sus necesidades	3 2	2.67	2.1	2.4	
	Enfermedad	2	Políticas internas de la empresa	2				
	Errores de digitación.	2	Políticas de selección del personal. Trabajo presión. Falta de capacitación.	3 2 2	2.67	2.1	2.4	
Facturador	Enfermedad	2	Políticas internas de la empresa	2	2.33	2.1	2.2	
	Falta de Responsabilidad	2	Políticas para seleccionar personal Falta de incentivos y atención a sus necesidades	3 2				
Sistema Power Street	Errores de código	1	Indebido control de pruebas realizadas. Falta de entorno informático de producción y pruebas Falta de Control de gestión de cambios	3 3 2	3	2.0	2.5	
	Fallos técnicos	2	No existe un generador eléctrico Problema con la red de computadores.	2 2				

			Fallo del servidor	3				
	Errores de usuario	2	Falta de capacitación. Trabajar a presión.	2 2				
	Fallos en el control de acceso de información	2	Falta de políticas de manipulación de claves.	2				
Inf. Del cliente (informativo)	Invención	3	Políticas de selección del personal. Capacitación.	3 2	2.67	2.7	2.6	
	Ilegibilidad de los datos	3	Políticas de selección del personal. Capacitación.	3 2				
Inf. Del cliente (pedidos)	Invención	3	Políticas de selección del personal. Capacitación.	3 2	2.67	2.7	2.6	
	Ilegibilidad de los datos	3	Políticas de selección del personal. Capacitación.	3 2				
Inf. Del vendedor	Invención	2	Políticas de selección del personal. Capacitación.	3 2	2.67	2.5	2.5	
	Ilegibilidad de los datos	3	Políticas de selección del personal. Capacitación.	3 2				
Libro de rutas	Mal concebidas	3	Deficiencia Organizacional	3	2.33	2.6	2.4	
	Errores de digitación	3	Políticas de selección del personal. Trabajo presión. Falta de capacitación.	3 2 2				
	Alteración.	2	Políticas de selección del personal	3				
Cliente	Invención	3	Políticas de selección del personal.	3	2.67	2.5	2.6	
	Ilegibilidad de los datos	3	Falta de capacitación.	2				
	Errores de digitación	2	Políticas de selección del personal. Trabajo presión. Falta de capacitación.	3 2 2				

Proceso: Pedidos a Clientes

Activos	Amenazas	Posibilidad Ocurrencia de la Amenaza	Vulnerabilidad	Posibilidad Que la amenaza Explote la vulnerabilidad	Valor Del Activo	Posible Ocurrencia de Amenaza y Vulnerabilidad	Total	Criticidad
Pockets	Robo del dispositivo	3	Inseguridad en las calles Falta de seguridad de la empresa Deficiencia organizacional	3 3 3	2.33	2.4	2.38	
	Fallo en el equipo	2	Falta de mantenimiento Equipos con suficiente horas de uso.	3 3				
	Falta de energía	2	No hay cargadores No prever la carga necesaria	2 2				
	Mal uso	2	Falta de capacitación	2				
computador	Fallo en el equipo	1	Falta de mantenimiento Falta de un buen entorno operativo	2 2	3	1.7	2.3	
	Falta de energía	2	Falta de un generador eléctrico Falta de un control operativo de los ups individuales.	2 2				
	Mal uso	1	Falta capacitación	2				
	Virus Informático	2	Políticas de seguridad No existe la adquisición de licencias de un antivirus	2 2				
Vendedores	Falta de Responsabilidad	2	Políticas para seleccionar personal Falta de incentivos y atención a sus necesidades	3 2	2.67	2.1	2.4	
	Enfermedad	2	Políticas internas de la empresa	2				
	Errores de digitación.	2	Políticas de selección del personal. Trabajo presión. Falta de capacitación.	3 2 2	2.67	2.1	2.4	
Facturador	Enfermedad	2	Políticas internas de la empresa	2	2.33	2.1	2.2	
	Falta de Responsabilidad	2	Políticas para seleccionar personal Falta de incentivos y atención a sus necesidades	3 2				
Bodeguero	Falta de respon	2	Políticas para seleccionar personal Falta de incentivos y	3 2	2.33	2.1	2.2	

	sabilidad		atención a sus necesidades					
	Enfermedad	2	Políticas internas de la empresa	2				
Sistema Power Street	Errores de código	1	Indebido control de pruebas realizadas. Falta de entorno informático de producción y pruebas Falta de Control de gestión de cambios	3 3 2	3	2.0	2.5	
	Fallos técnicos	2	No existe un generador eléctrico Problema con la red de computadores. Fallo del servidor	2 2 3				
	Errores de usuario	2	Falta de capacitación. Trabajar a presión.	2 2				
	Fallos en el control de acceso de información	2	Falta de políticas de manipulación de claves.	2				
Inf. Del cliente (informativo)	Invención	3	Políticas de selección del personal. Capacitación.	3 2	2.67	2.7	2.6	
	Ilegibilidad de los datos	3	Políticas de selección del personal. Capacitación.	3 2				
Inf. Del cliente (pedidos)	Invención	3	Políticas de selección del personal. Capacitación.	3 2	2.67	2.7	2.6	
	Ilegibilidad de los datos	3	Políticas de selección del personal. Capacitación.	3 2				
Inf. Del vendedor	Invención	2	Políticas de selección del personal. Capacitación.	3 2	2.67	2.5	2.5	
	Ilegibilidad de los datos	3	Políticas de selección del personal. Capacitación.	3 2				
Libro de rutas	Mal concebidas	3	Deficiencia Organizacional	3	2.33	2.6	2.4	
	Errores de digitación	3	Políticas de selección del personal. Trabajo presión. Falta de capacitación.	3 2 2				
	Alteración.	2	Políticas de selección del personal	3				
Cliente	Invención	3	Políticas de selección del personal.	3	2.67	2.5	2.6	

	Ilegibilidad de los datos	3	Falta de capacitación.	2				
	Errores de digitación	2	Políticas de selección del personal. Trabajo presión. Falta de capacitación.	3 2 2				

Proceso: Facturación

Activos	**Amenazas**	**Posibilidad Ocurrencia de la Amenaza**	**Vulnerabilidad**	**Posibilidad Que la amenaza Explote la vulnerabilidad**	**Valor Del Activo**	**Posible Ocurrencia de Amenaza y Vulnerabilidad**	**Total**	**Criticidad**
Pockets	Robo del dispositivo	3	Inseguridad en las calles Falta de seguridad de la empres Deficiencia organizacional	3 3 3	2.33	2.4	2.3	
	Fallo en el equipo	2	Falta de mantenimiento Equipos con suficiente horas de uso.	3 3				
	Falta de energía	2	No hay cargadores No prever la carga necesaria	2 2				
	Mal uso	2	Falta de capacitación	2				
computador	Fallo en el equipo	1	Falta de mantenimiento Falta de un buen entorno operativo	2 2	3	1.7	2.3	
	Falta de energía	2	Falta de un generador eléctrico Falta de un control operativo de los ups individuales.	2 2				
	Mal uso	1	Falta capacitación	2				
	Virus Informático	2	Políticas de seguridad No existe la adquisición de licencias de un antivirus	2 2				
Vendedores	Falta de Responsabilidad	2	Políticas para seleccionar personal Falta de incentivos y atención a sus necesidades	3 2	2.67	2.1	2.4	
	Enfermedad	2	Políticas internas de la empresa	2				
Facturador	Enfermedad	2	Políticas internas de la empresa	2	2.33	2.1	2.2	
	Falta de Responsabilidad	2	Políticas para seleccionar personal Falta de incentivos y atención a sus necesidades	3 2				
Bodega	Falta de	2	Políticas para seleccionar	3	2.33	2.1	2.2	

	responsabilidad		personal Falta de incentivos y atención a sus necesidades	2				
	Enfermedad	2	Políticas internas de la empresa	2				
Sistema power Street	Errores de código	1	Indebido control de pruebas realizadas. Falta de entorno informático de producción y pruebas Falta de Control de gestión de cambios	3 3 2	3	2.0	2.5	
	Fallos técnicos	2	No existe un generador eléctrico Problema con la red de computadores. Fallo del servidor	2 2 3				
	Errores de usuario	2	Falta de capacitación. Trabajar a presión.	2 2				
	Fallos en el control de acceso de información	2	Falta de políticas de manipulación de claves.	2				
Inf. Del cliente (informativo)	Invención	3	Políticas de selección del personal. Capacitación.	3 2	2.67	2.7	2.7	
	Ilegibilidad de los datos	3	Políticas de selección del personal. Capacitación.	3 2				
Inf. Del cliente (pedidos)	Invención	3	Políticas de selección del personal. Capacitación.	3 2	2.67	2.7	2.7	
	Ilegibilidad de los datos	3	Políticas de selección del personal. Capacitación.	3 2				
Inf. Del vendedor	Invención	2	Políticas de selección del personal. Capacitación.	3 2	2.67	2.5	2.5	
	Ilegibilidad de los datos	3	Políticas de selección del personal. Capacitación.	3 2				
Libro de rutas	Mal concebidas	3	Deficiencia Organizacional	3	2.33	2.6	2.4	
	Errores de digitación	3	Políticas de selección del personal. Trabajo presión. Falta de capacitación.	3 2 2				
	Alteración.	2	Políticas de selección del personal	3				
Vendedor	Errores de	2	Políticas de selección del personal.	3 2	2.67	2.1	2.4	

	digitación.		Trabajo presión. Falta de capacitación.	2				
Cliente	Invención	3	Políticas de selección del personal.	3	2.67	2.5	2.6	
	Ilegibilidad de los datos	3	Falta de capacitación.	2				
	Errores de digitación	2	Políticas de selección del personal. Trabajo presión. Falta de capacitación.	3 2 2				
Facturadores	Errores de Digitaciòn	2	Trabajo bajo presión Capacitación	2 2	3	2	2.5	

Proceso: Crédito

Activos	**Amenazas**	**Posibilidad Ocurrencia de la Amenaza**	**Vulnerabilidad**	**Posibilidad Que la amenaza Explote la vulnerabilidad**	**Valor Del Activo**	**Posible Ocurrencia de Amenaza y Vulnerabilidad**	**Total**	**Criticidad**
computador	Fallo en el equipo	1	Falta de mantenimiento Falta de un buen entorno operativo	2 2	3	1.7	2.3	
	Falta de energía	2	Falta de un generador eléctrico Falta de un control operativo de los ups individuales.	2 2				
	Mal uso	1	Falta capacitación	2				
	Virus Informático	2	Políticas de seguridad No existe la adquisición de licencias de un antivirus	2 2				
Vendedores	Falta de Responsabilidad	2	Políticas para seleccionar personal Falta de incentivos y atención a sus necesidades	3 2	2.67	2.1	2.4	
	Enfermedad	2	Políticas internas de la empresa	2				
Facturador	Enfermedad	2	Políticas internas de la empresa	2	3	2.1	2.5	
	Falta de Responsabilidad	2	Políticas para seleccionar personal Falta de incentivos y atención a sus necesidades	3 2				
Crédito	Enfermedad	2	Políticas internas de la empresa	2	3	2.1	2.5	

	Falta de Responsabilidad	2	Políticas para seleccionar personal Falta de incentivos y atención a sus necesidades	3 2				
Sistema Power Street	Errores de código	1	Indebido control de pruebas realizadas. Falta de entorno informático de producción y pruebas Falta de Control de gestión de cambios	3 3 2	2	2.0	2.0	
	Fallos técnicos	2	No existe un generador eléctrico Problema con la red de computadores. Fallo del servidor	2 2 3				
	Errores de usuario	2	Falta de capacitación. Trabajar a presión.	2 2				
	Fallos en el control de acceso de información	2	Falta de políticas de manipulación de claves.	2				
Sistema Visual Fac	Errores de código	1	Indebido control de pruebas realizadas. Falta de entorno informático de producción y pruebas Falta de Control de gestión de cambios	3 3 2	3	2.0	2.5	
	Fallos técnicos	2	No existe un generador eléctrico Problema con la red de computadores. Fallo del servidor	2 2 3				
	Errores de usuario	2	Falta de capacitación. Trabajar a presión.	2 2				
	Fallos en el control de acceso de información	2	Falta de políticas de manipulación de claves.	2				
Cancelaciones	Invención	2	Políticas de selección del personal. Capacitación.	3 2	3	2.2	2.6	
	Errores de usuario	2	Políticas de selección del personal. Capacitación.	3 2				
Libro de rutas	Mal concebidas	3	Deficiencia Organizacional	3	2.33	2.6	2.4	
	Errores de digitació	3	Políticas de selección del personal. Trabajo presión.	3 2				

	n		Falta de capacitación.	2				
	Alteración.	2	Políticas de selección del personal	3				
Vendedor	Errores de digitación.	2	Políticas de selección del personal. Trabajo presión. Falta de capacitación.	3 2 2	2.67	2.1	2.4	
Cliente	Invención	3	Políticas de selección del personal.	3	2.67	2.5	2.6	
	Ilegibilidad de los datos	3	Falta de capacitación.	2				
	Errores de digitación	2	Políticas de selección del personal. Trabajo presión. Falta de capacitación.	3 2 2				
Factura	Errores de Digitación	2	Trabajo bajo presión Capacitación	2 2	3	2	2.5	

5.4 Tratamiento del Riesgo

En este punto se categorizan los riesgos e identifican cuales deberían ser tratados primero o más exhaustivamente. Se debe escoger, a la vista de los resultados, cual es el nivel de riesgo que la organización está dispuesta a tolerar (Criticidad Media), de manera que por debajo de ese nivel el riesgo es aceptable y por encima no lo será y se tomará alguna decisión al respecto.

Hay cuatro tipos de decisiones para tratar los riesgos que se consideran no aceptables (Criticidad Alta):

Asumirlo

Aceptar que no se puede hacer nada y por lo tanto se asume ese riesgo y se continúa operando tal como se ha venido haciendo.

Eliminarlo

Se elimina el riesgo, normalmente sólo se puede hacer eliminando el activo que lo genera, por ello esta opción no suele ser viable.

Transferirlo

El riesgo se traspasa a otra organización, por ejemplo mediante un seguro.

Mitigarlo

Es decir, reducir el riesgo, normalmente aplicando controles de seguridad. Es una de las opciones más habituales.

Para cada riesgo (criticidad Alta) identificado en la evaluación de riesgos la gerencia de OROTONI Cía. Ltda., ha decidido mitigarlo.

5.5 Selección de Controles

Teniendo en cuenta los riesgos detectados en los pasos anteriores, se ha decidido implantar las siguientes medidas de seguridad (Tomados de la norma ISO/IEC 27001:2005 Anexo A.).

5.6 Enunciado de Aplicabilidad

Proceso Mantenimiento de Tablas

Activo	Dominio		Objetivo de Control		Control		Aplicación	Justificación
Vendedores	A.8	Seguridad de los Recursos Humanos	A.8.1	Antes del Empleo	A.8.1.1	Roles y Responsabilidades	SI	Para asegurar que los empleados entiendan sus responsabilidades.
					A.8.1.2	Selección	SI	Para garantizar que los empleados sean los más adecuados para los roles.
					A.8.1.3	Términos y condiciones de empleo	SI	Permitirá reducir los riesgos de robo, fraude o mal uso de los medios.
			A.8.2	Durante el empleo	A.8.2.1	Gestión de responsabilidades	SI	Con el fin de que los empleados estén al tanto de sus responsabilidades y apliquen las políticas de seguridad de la información de la organización.

					A.8.2.2	Capacitación en educación en seguridad de la información	SI	Para asegurar que los empleados estén al tanto de las amenazas e inquietudes sobre la seguridad de la información
					A.8.2.3	Proceso disciplinario	SI	Como apoyo a la concienciación a la seguridad de la información.
			A.8.3	Terminación o cambio de empleo	A.8.3.1	Responsabilidades de terminación	SI	Asegurar que los empleados salgan de la organización de una manera segura.
					A.8.3.2	Devolución de activos	SI	
					A.8.3.3	Eliminación de derechos de acceso	SI	
Sistema Power Street	A.7	Gestión de activos	A.7.1	Responsabilidad por los activos	A.7.1.1	Inventario de activos	SI	Lograr y mantener la protección apropiada de los activos organizacionales

					A.7.1.2	Propiedad de los activos	SI	
					A.7.1.3	Uso aceptable de los activos	SI	
	A.10	Gestión de las comunicaciones y operaciones	A.10.1	Procedimientos y responsabilidades operacionales	A.10.1.1	Procedimientos de operación documentados	SI	Asegurar la operación correcta y segura de los medios de procesamiento de la información
					A.10.1.2	Gestión de cambio	SI	
					A.10.1.3	Segregación de deberes	SI	
					A.10.1.4	Separación de los medios de desarrollo y operacionales	SI	

			A.10.3	Planeación y aceptación del sistema	A.10.3.1	Gestión de la capacidad	SI	Minimizar el riesgo de fallas en los sistemas
					A.10.3.2	Aceptación del sistema	SI	
			A.10.5	Respaldo (backup)	A.10.5.1	Backup o respaldo de la información	SI	Para mantener la integridad y disponibilidad de los servicios de procesamiento de información y comunicaciones
			A.10.8	Intercambio de información	A.10.8.1	Procedimientos y políticas de información y software	SI	Para proteger el intercambio de información
					A.10.8.2	Acuerdos de intercambio	SI	Para garantizar la seguridad de la información y software intercambiados
					A.10.8.3	Medios físicos en tránsito	SI	

					A.10.8.4	Mensajes electrónicos	SI	
					A.10.8.5	Sistemas de información comercial	SI	Para proteger la información asociada con la interconexión de los sistemas de información comercial
			A.10.10	Monitoreo	A.10.10.2	Protección de la información del registro	SI	Con la finalidad de detectar actividades de procesamiento de información no autorizadas
					A.10.10.5	Registro de fallas	SI	
					A.10.10.6	Sincronización de relojes	SI	
	A.11	Control de Acceso	A.11.1	Requerimiento comercial para el control de acceso	A.11.1.1	Política de control de acceso	SI	Controlar acceso a la información

			A.11.2	Gestión del acceso del usuario	A.11.2.1	Inscripción del usuario		Asegurar el acceso a usuario al usuario autorizado y evitar el acceso no autorizado a los sistemas de información
					A.11.2.2	Gestión de privilegios	SI	
					A.11.2.3	Gestión de la clave del usuario	SI	
					A.11.2.4	Revisión de los derechos de acceso al usuario	SI	
			A.11.3	Responsabilidades del usuario	A.11.3.1	Uso de clave	SI	Así se evitará el acceso de usuarios no autorizados, también se evitará el robo de la información y los medios de procesamiento de la información
					A.11.3.2	Equipo de usuario desatendido	SI	

					A.11.3.3	Política de pantalla y escritorio limpio	SI	
			A.11.6	Control de acceso a la información y aplicación	A.11.6.1	Restricción al acceso a la información	SI	Para evitar el acceso no autorizado a la información mantenida en los sistemas de aplicación
					A.11.6.2	Aislamiento del sistema sensible	SI	
	A.12	Adquisición, desarrollo y mantenimiento de los sistemas de información	A.12.1	Requerimientos de seguridad de los sistemas	A.12.1.1	Análisis y especificación de los requerimientos de seguridad	SI	Asegurar que la seguridad sea una parte integral de los sistemas de información
			A.12.2	Procesamiento correcto en las aplicaciones	A.12.2.1	Validación de la data de insumo	SI	Permite asegurar que la data sea correcta y apropiada
					A.12.2.2	Control de procesamiento interno	SI	Para detectar cualquier corrupción de la información

					A.12.2.3	Integridad del mensaje	SI	Para asegurar la autenticidad y protección de la integridad de mensaje en las aplicaciones
					A.12.2.4	Validación de la data de output	SI	Asegurar que el procesamiento de la información almacenada sea correcto y apropiado para las circunstancias
			A.12.4	Seguridad de los archivos del sistema	A.12.4.1	Control de software operacional	SI	Para garantizar la seguridad de los archivos del sistema
					A.12.4.2	Protección de la data de prueba del sistema	SI	
					A.12.4.3	Control de acceso al código fuente del programa	SI	
			A.12.5	Seguridad de los procesos de desarrollo y soporte	A.12.5.1	Procedimiento de control de cambio	SI	Para mantener la seguridad del software e información del sistema de aplicación

					A.12.5.2	Revisión técnica de las aplicaciones después de cambios en el sistema operativo	SI	
					A.12.5.3	Restricciones sobre los cambios en los paquetes de software	SI	
			A.12.6	Gestión de vulnerabilidad técnica	A.12.6.1	Control de vulnerabilidades técnicas	SI	Para reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas publicadas

Proceso Pedidos a Clientes

Activo	Dominio		Objetivo de Control		Control		Aplicación	Justificación
Vendedores	A.8	Seguridad de los Recursos Humanos	A.8.1	Antes del Empleo	A.8.1.1	Roles y Responsabilidades	SI	Para asegurar que los empleados entiendan sus responsabilidades.
					A.8.1.2	Selección	SI	Para garantizar que los empleados sean los más adecuados para los roles.
					A.8.1.3	Términos y condiciones de empleo	SI	Permitirá reducir los riesgos de robo, fraude o mal uso de los medios.
			A.8.2	Durante el empleo	A.8.2.1	Gestión de responsabilidades	SI	Con el fin de que los empleados estén al tanto de sus responsabilidades y apliquen las políticas de seguridad de la información de la organización.

					A.8.2.2	Capacitación en educación en seguridad de la información	SI	Para asegurar que los empleados estén al tanto de las amenazas e inquietudes sobre la seguridad de la información
					A.8.2.3	Proceso disciplinario	SI	Como apoyo a la concienciación a la seguridad de la información.
			A.8.3	Terminación o cambio de empleo	A.8.3.1	Responsabilidades de terminación	SI	Asegurar que los empleados salgan de la organización de una manera segura.
					A.8.3.2	Devolución de activos	SI	
					A.8.3.3	Eliminación de derechos de acceso	SI	
Sistema Power Street	A.7	Gestión de activos	A.7.1	Responsabilidad por los activos	A.7.1.1	Inventario de activos	SI	Lograr y mantener la protección apropiada de los activos organizacionales

					A.7.1.2	Propiedad de los activos	SI	
					A.7.1.3	Uso aceptable de los activos	SI	
	A.10	Gestión de las comunicaciones y operaciones	A.10.1	Procedimientos y responsabilidades operacionales	A.10.1.1	Procedimientos de operación documentados	SI	Asegurar la operación correcta y segura de los medios de procesamiento de la información
					A.10.1.2	Gestión de cambio	SI	
					A.10.1.3	Segregación de deberes	SI	
					A.10.1.4	Separación de los medios de desarrollo y operacionales	SI	

			A.10.3	Planeación y aceptación del sistema	A.10.3.1	Gestión de la capacidad	SI	Minimizar el riesgo de fallas en los sistemas
					A.10.3.2	Aceptación del sistema	SI	
			A.10.5	Respaldo (backup)	A.10.5.1	Backup o respaldo de la información	SI	Para mantener la integridad y disponibilidad de los servicios de procesamiento de información y comunicaciones
			A.10.8	Intercambio de información	A.10.8.1	Procedimientos y políticas de información y software	SI	Para proteger el intercambio de información
					A.10.8.2	Acuerdos de intercambio	SI	Para garantizar la seguridad de la información y software intercambiados
					A.10.8.3	Medios físicos en tránsito	SI	

					A.10.8.4	Mensajes electrónicos	SI	
					A.10.8.5	Sistemas de información comercial	SI	Para proteger la información asociada con la interconexión de los sistemas de información comercial
			A.10.10	Monitoreo	A.10.10.2	Protección de la información del registro	SI	Con la finalidad de detectar actividades de procesamiento de información no autorizadas
					A.10.10.5	Registro de fallas	SI	
					A.10.10.6	Sincronización de relojes	SI	
	A.11	Control de Acceso	A.11.1	Requerimiento comercial para el control de acceso	A.11.1.1	Política de control de acceso	SI	Controlar acceso a la información

			A.11.2	Gestión del acceso del usuario	A.11.2.1	Inscripción del usuario		Asegurar el acceso a usuario al usuario autorizado y evitar el acceso no autorizado a los sistemas de información
					A.11.2.2	Gestión de privilegios	SI	
					A.11.2.3	Gestión de la clave del usuario	SI	
					A.11.2.4	Revisión de los derechos de acceso al usuario	SI	
			A.11.3	Responsabilidades del usuario	A.11.3.1	Uso de clave	SI	Así se evitará el acceso de usuarios no autorizados, también se evitará el robo de la información y los medios de procesamiento de la información
					A.11.3.2	Equipo de usuario desatendido	SI	

					A.11.3.3	Política de pantalla y escritorio limpio	SI	
			A.11.6	Control de acceso a la información y aplicación	A.11.6.1	Restricción al acceso a la información	SI	Para evitar el acceso no autorizado a la información mantenida en los sistemas de aplicación
					A.11.6.2	Aislamiento del sistema sensible	SI	
	A.12	Adquisición, desarrollo y mantenimiento de los sistemas de información	A.12.1	Requerimientos de seguridad de los sistemas	A.12.1.1	Análisis y especificación de los requerimientos de seguridad	SI	Asegurar que la seguridad sea una parte integral de los sistemas de información
			A.12.2	Procesamiento correcto en las aplicaciones	A.12.2.1	Validación de la data de insumo	SI	Permite asegurar que la data sea correcta y apropiada
					A.12.2.2	Control de procesamiento interno	SI	Para detectar cualquier corrupción de la información

					A.12.2.3	Integridad del mensaje	SI	Para asegurar la autenticidad y protección de la integridad de mensaje en las aplicaciones
					A.12.2.4	Validación de la data de output	SI	Asegurar que el procesamiento de la información almacenada sea correcto y apropiado para las circunstancias
			A.12.4	Seguridad de los archivos del sistema	A.12.4.1	Control de software operacional	SI	Para garantizar la seguridad de los archivos del sistema
					A.12.4.2	Protección de la data de prueba del sistema	SI	
					A.12.4.3	Control de acceso al código fuente del programa	SI	
			A.12.5	Seguridad de los procesos de desarrollo y soporte	A.12.5.1	Procedimiento de control de cambio	SI	Para mantener la seguridad del software e información del sistema de aplicación

					A.12.5.2	Revisión técnica de las aplicaciones después de cambios en el sistema operativo	SI	
					A.12.5.3	Restricciones sobre los cambios en los paquetes de software	SI	
			A.12.6	Gestión de vulnerabilidad técnica	A.12.6.1	Control de vulnerabilidades técnicas	SI	Para reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas publicadas
Inf. Del Cliente (informativo)	A.7	Gestión de activos	A.7.1	Responsabilidad por los activos	A.7.1.1	Inventario de activos	SI	Lograr y mantener la protección apropiada de los activos organizacionales
					A.7.1.2	Propiedad de los activos	SI	
					A.7.1.3	Uso aceptable de los activos	SI	

			A.7.2	Clasificación de la información	A.7.2.1	Lineamientos de clasificación	SI	Asegurar que la información reciba un nivel de protección apropiado
					A.7.2.2	Etiquetado y manejo de la información	SI	
Inf. Del cliente (pedidos)	A.7	Gestión de activos	A.7.1	Responsabilidad por los activos	A.7.1.1	Inventario de activos	SI	Lograr y mantener la protección apropiada de los activos organizacionales
					A.7.1.2	Propiedad de los activos	SI	
					A.7.1.3	Uso aceptable de los activos	SI	
			A.7.2	Clasificación de la información	A.7.2.1	Lineamientos de clasificación	SI	Asegurar que la información reciba un nivel de protección apropiado

					A.7.2.2	Etiquetado y manejo de la información	SI	
Inf. Del vendedor	A.7	Gestión de activos	A.7.1	Responsabilidad por los activos	A.7.1.1	Inventario de activos	SI	Lograr y mantener la protección apropiada de los activos organizacionales
					A.7.1.2	Propiedad de los activos	SI	
					A.7.1.3	Uso aceptable de los activos	SI	
			A.7.2	Clasificación de la información	A.7.2.1	Lineamientos de clasificación	SI	Asegurar que la información reciba un nivel de protección apropiado
					A.7.2.2	Etiquetado y manejo de la información	SI	

Libro de rutas	A.7	Gestión de activos	A.7.1	Responsabilidad por los activos	A.7.1.1	Inventario de activos	SI	Lograr y mantener la protección apropiada de los activos organizacionales
					A.7.1.2	Propiedad de los activos	SI	
					A.7.1.3	Uso aceptable de los activos	SI	
			A.7.2	Clasificación de la información	A.7.2.1	Lineamientos de clasificación	SI	Asegurar que la información reciba un nivel de protección apropiado
					A.7.2.2	Etiquetado y manejo de la información	SI	

Proceso Facturación

Activo	Dominio		Objetivo de Control		Control		Aplicación	Justificación
Vendedores	A.8	Seguridad de los Recursos Humanos	A.8.1	Antes del Empleo	A.8.1.1	Roles y Responsabilidades	SI	Para asegurar que los empleados entiendan sus responsabilidades.
					A.8.1.2	Selección	SI	Para garantizar que los empleados sean los más adecuados para los roles.
					A.8.1.3	Términos y condiciones de empleo	SI	Permitirá reducir los riesgos de robo, fraude o mal uso de los medios.
			A.8.2	Durante el empleo	A.8.2.1	Gestión de responsabilidades	SI	Con el fin de que los empleados estén al tanto de sus responsabilidades y apliquen las políticas de seguridad de la información de la organización.
					A.8.2.2	Capacitación en educación en seguridad de la información	SI	Para asegurar que los empleados estén al tanto de las amenazas e inquietudes sobre la seguridad de la información

					A.8.2.3	Proceso disciplinario	SI	Como apoyo a la concienciación a la seguridad de la información.
			A.8.3	Terminación o cambio de empleo	A.8.3.1	Responsabilidades de terminación	SI	Asegurar que los empleados salgan de la organización de una manera segura.
					A.8.3.2	Devolución de activos	SI	
					A.8.3.3	Eliminación de derechos de acceso	SI	
Sistema Power Street	A.7	Gestión de activos	A.7.1	Responsabilidad por los activos	A.7.1.1	Inventario de activos	SI	Lograr y mantener la protección apropiada de los activos organizacionales
					A.7.1.2	Propiedad de los activos	SI	

					A.7.1.3	Uso aceptable de los activos	SI	
	A.10	Gestión de las comunicaciones y operaciones	A.10.1	Procedimientos y responsabilidades operacionales	A.10.1.1	Procedimientos de operación documentados	SI	Asegurar la operación correcta y segura de los medios de procesamiento de la información
					A.10.1.2	Gestión de cambio	SI	
					A.10.1.3	Segregación de deberes	SI	
					A.10.1.4	Separación de los medios de desarrollo y operacionales	SI	
			A.10.3	Planeación y aceptación del sistema	A.10.3.1	Gestión de la capacidad	SI	Minimizar el riesgo de fallas en los sistemas

					A.10.3.2	Aceptación del sistema	SI	
			A.10.5	Respaldo (backup)	A.10.5.1	Backup o respaldo de la información	SI	Para mantener la integridad y disponibilidad de los servicios de procesamiento de información y comunicaciones
			A.10.8	Intercambio de información	A.10.8.1	Procedimientos y políticas de información y software	SI	Para proteger el intercambio de información
					A.10.8.2	Acuerdos de intercambio	SI	Para garantizar la seguridad de la información y software intercambiados
					A.10.8.3	Medios físicos en tránsito	SI	
					A.10.8.4	Mensajes electrónicos	SI	

					A.10.8.5	Sistemas de información comercial	SI	Para proteger la información asociada con la interconexión de los sistemas de información comercial
			A.10.10	Monitoreo	A.10.10.2	Protección de la información del registro	SI	Con la finalidad de detectar actividades de procesamiento de información no autorizadas
					A.10.10.5	Registro de fallas	SI	
					A.10.10.6	Sincronización de relojes	SI	
	A.11	Control de Acceso	A.11.1	Requerimiento comercial para el control de acceso	A.11.1.1	Política de control de acceso	SI	Controlar acceso a la información
			A.11.2	Gestión del acceso del usuario	A.11.2.1	Inscripción del usuario		Asegurar el acceso a usuario al usuario autorizado y evitar el acceso no autorizado a los sistemas de información

					A.11.2.2	Gestión de privilegios	SI	
					A.11.2.3	Gestión de la clave del usuario	SI	
					A.11.2.4	Revisión de los derechos de acceso al usuario	SI	
			A.11.3	Responsabilidades del usuario	A.11.3.1	Uso de clave	SI	Así se evitará el acceso de usuarios no autorizados, también se evitará el robo de la información y los medios de procesamiento de la información
					A.11.3.2	Equipo de usuario desatendido	SI	
					A.11.3.3	Política de pantalla y escritorio limpio	SI	

			A.11.6	Control de acceso a la información y aplicación	A.11.6.1	Restricción al acceso a la información	SI	Para evitar el acceso no autorizado a la información mantenida en los sistemas de aplicación
					A.11.6.2	Aislamiento del sistema sensible	SI	
	A.12	Adquisición, desarrollo y mantenimiento de los sistemas de información	A.12.1	Requerimientos de seguridad de los sistemas	A.12.1.1	Análisis y especificación de los requerimientos de seguridad	SI	Asegurar que la seguridad sea una parte integral de los sistemas de información
			A.12.2	Procesamiento correcto en las aplicaciones	A.12.2.1	Validación de la data de insumo	SI	Permite asegurar que la data sea correcta y apropiada
					A.12.2.2	Control de procesamiento interno	SI	Para detectar cualquier corrupción de la información
					A.12.2.3	Integridad del mensaje	SI	Para asegurar la autenticidad y protección de la integridad de mensaje en las aplicaciones

					A.12.2.4	Validación de la data de output	SI	Asegurar que el procesamiento de la información almacenada sea correcto y apropiado para las circunstancias
			A.12.4	Seguridad de los archivos del sistema	A.12.4.1	Control de software operacional	SI	Para garantizar la seguridad de los archivos del sistema
					A.12.4.2	Protección de la data de prueba del sistema	SI	
					A.12.4.3	Control de acceso al código fuente del programa	SI	
			A.12.5	Seguridad de los procesos de desarrollo y soporte	A.12.5.1	Procedimiento de control de cambio	SI	Para mantener la seguridad del software e información del sistema de aplicación
					A.12.5.2	Revisión técnica de las aplicaciones después de cambios en el sistema operativo	SI	

					A.12.5.3	Restricciones sobre los cambios en los paquetes de software	SI	
			A.12.6	Gestión de vulnerabilidad técnica	A.12.6.1	Control de vulnerabilidades técnicas	SI	Para reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas publicadas
Inf. Del Cliente (informativo)	A.7	Gestión de activos	A.7.1	Responsabilidad por los activos	A.7.1.1	Inventario de activos	SI	Lograr y mantener la protección apropiada de los activos organizacionales
					A.7.1.2	Propiedad de los activos	SI	
					A.7.1.3	Uso aceptable de los activos	SI	
			A.7.2	Clasificación de la información	A.7.2.1	Lineamientos de clasificación	SI	Asegurar que la información reciba un nivel de protección apropiado

					A.7.2.2	Etiquetado y manejo de la información	SI	
Inf. Del cliente (pedidos)	A.7	Gestión de activos	A.7.1	Responsabilidad por los activos	A.7.1.1	Inventario de activos	SI	Lograr y mantener la protección apropiada de los activos organizacionales
					A.7.1.2	Propiedad de los activos	SI	
					A.7.1.3	Uso aceptable de los activos	SI	
			A.7.2	Clasificación de la información	A.7.2.1	Lineamientos de clasificación	SI	Asegurar que la información reciba un nivel de protección apropiado
					A.7.2.2	Etiquetado y manejo de la información	SI	

Inf. Del vendedor	A.7	Gestión de activos	A.7.1	Responsabilidad por los activos	A.7.1.1	Inventario de activos	SI	Lograr y mantener la protección apropiada de los activos organizacionales
					A.7.1.2	Propiedad de los activos	SI	
					A.7.1.3	Uso aceptable de los activos	SI	
			A.7.2	Clasificación de la información	A.7.2.1	Lineamientos de clasificación	SI	Asegurar que la información reciba un nivel de protección apropiado
					A.7.2.2	Etiquetado y manejo de la información	SI	
Libro de rutas	A.7	Gestión de activos	A.7.1	Responsabilidad por los activos	A.7.1.1	Inventario de activos	SI	Lograr y mantener la protección apropiada de los activos organizacionales

					A.7.1.2	Propiedad de los activos	SI	
					A.7.1.3	Uso aceptable de los activos	SI	
			A.7.2	Clasificación de la información	A.7.2.1	Lineamientos de clasificación	SI	Asegurar que la información reciba un nivel de protección apropiado
					A.7.2.2	Etiquetado y manejo de la información	SI	

Proceso Crédito

Activo	Dominio		Objetivo de Control		Control		Aplicación	Justificación
Vendedores	A.8	Seguridad de los Recursos Humanos	A.8.1	Antes del Empleo	A.8.1.1	Roles y Responsabilidades	SI	Para asegurar que los empleados entiendan sus responsabilidades.
					A.8.1.2	Selección	SI	Para garantizar que los empleados sean los más adecuados para los roles.
					A.8.1.3	Términos y condiciones de empleo	SI	Permitirá reducir los riesgos de robo, fraude o mal uso de los medios.
			A.8.2	Durante el empleo	A.8.2.1	Gestión de responsabilidades	SI	Con el fin de que los empleados estén al tanto de sus responsabilidades y apliquen las políticas de seguridad de la información de la organización.
					A.8.2.2	Capacitación en educación en seguridad de la información	SI	Para asegurar que los empleados estén al tanto de las amenazas e inquietudes sobre la seguridad de la información
					A.8.2.3	Proceso disciplinario	SI	Como apoyo a la concienciación a la seguridad de la información.

			A.8.3	Terminación o cambio de empleo	A.8.3.1	Responsabilidades de terminación	SI	Asegurar que los empleados salgan de la organización de una manera segura.
					A.8.3.2	Devolución de activos	SI	
					A.8.3.3	Eliminación de derechos de acceso	SI	
Facturador	A.8	Seguridad de los Recursos Humanos	A.8.1	Antes del Empleo	A.8.1.1	Roles y Responsabilidades	SI	Para asegurar que los empleados entiendan sus responsabilidades.
					A.8.1.2	Selección	SI	Para garantizar que los empleados sean los más adecuados para los roles.
					A.8.1.3	Términos y condiciones de empleo	SI	Permitirá reducir los riesgos de robo, fraude o mal uso de los medios.

			A.8.2	Durante el empleo	A.8.2.1	Gestión de responsabilidades	SI	Con el fin de que los empleados estén al tanto de sus responsabilidades y apliquen las políticas de seguridad de la información de la organización.
					A.8.2.2	Capacitación en educación en seguridad de la información	SI	Para asegurar que los empleados estén al tanto de las amenazas e inquietudes sobre la seguridad de la información
					A.8.2.3	Proceso disciplinario	SI	Como apoyo a la concienciación a la seguridad de la información.
			A.8.3	Terminación o cambio de empleo	A.8.3.1	Responsabilidades de terminación	SI	Asegurar que los empleados salgan de la organización de una manera segura.
					A.8.3.2	Devolución de activos	SI	
					A.8.3.3	Eliminación de derechos de acceso	SI	

Crédito	A.8	Seguridad de los Recursos Humanos	A.8.1	Antes del Empleo	A.8.1.1	Roles y Responsabilidades	SI	Para asegurar que los empleados entiendan sus responsabilidades.
					A.8.1.2	Selección	SI	Para garantizar que los empleados sean los más adecuados para los roles.
					A.8.1.3	Términos y condiciones de empleo	SI	Permitirá reducir los riesgos de robo, fraude o mal uso de los medios.
			A.8.2	Durante el empleo	A.8.2.1	Gestión de responsabilidades	SI	Con el fin de que los empleados estén al tanto de sus responsabilidades y apliquen las políticas de seguridad de la información de la organización.
					A.8.2.2	Capacitación en educación en seguridad de la información	SI	Para asegurar que los empleados estén al tanto de las amenazas e inquietudes sobre la seguridad de la información
					A.8.2.3	Proceso disciplinario	SI	Como apoyo a la concienciación a la seguridad de la información.

			A.8.3	Terminación o cambio de empleo	A.8.3.1	Responsabilidades de terminación	SI	Asegurar que los empleados salgan de la organización de una manera segura.
					A.8.3.2	Devolución de activos	SI	
					A.8.3.3	Eliminación de derechos de acceso	SI	
Sistema Visual Fac	A.7	Gestión de activos	A.7.1	Responsabilidad por los activos	A.7.1.1	Inventario de activos	SI	Lograr y mantener la protección apropiada de los activos organizacionales
					A.7.1.2	Propiedad de los activos	SI	
					A.7.1.3	Uso aceptable de los activos	SI	

	A.10	Gestión de las comunicaciones y operaciones	A.10.1	Procedimientos y responsabilidades operacionales	A.10.1.1	Procedimientos de operación documentados	SI	Asegurar la operación correcta y segura de los medios de procesamiento de la información
					A.10.1.2	Gestión de cambio	SI	
					A.10.1.3	Segregación de deberes	SI	
					A.10.1.4	Separación de los medios de desarrollo y operacionales	SI	
			A.10.3	Planeación y aceptación del sistema	A.10.3.1	Gestión de la capacidad	SI	Minimizar el riesgo de fallas en los sistemas
					A.10.3.2	Aceptación del sistema	SI	

			A.10.5	Respaldo (backup)	A.10.5.1	Backup o respaldo de la información	SI	Para mantener la integridad y disponibilidad de los servicios de procesamiento de información y comunicaciones
			A.10.8	Intercambio de información	A.10.8.1	Procedimientos y políticas de información y software	SI	Para proteger el intercambio de información
					A.10.8.2	Acuerdos de intercambio	SI	Para garantizar la seguridad de la información y software intercambiados
					A.10.8.3	Medios físicos en tránsito	SI	
					A.10.8.4	Mensajes electrónicos	SI	
					A.10.8.5	Sistemas de información comercial	SI	Para proteger la información asociada con la interconexión de los sistemas de información comercial

			A.10.10	Monitoreo	A.10.10.2	Protección de la información del registro	SI	Con la finalidad de detectar actividades de procesamiento de información no autorizadas
					A.10.10.5	Registro de fallas	SI	
					A.10.10.6	Sincronización de relojes	SI	
	A.11	Control de Acceso	A.11.1	Requerimiento comercial para el control de acceso	A.11.1.1	Política de control de acceso	SI	Controlar acceso a la información
			A.11.2	Gestión del acceso del usuario	A.11.2.1	Inscripción del usuario		Asegurar el acceso a usuario al usuario autorizado y evitar el acceso no autorizado a los sistemas de información
					A.11.2.2	Gestión de privilegios	SI	

					A.11.2.3	Gestión de la clave del usuario	SI	
					A.11.2.4	Revisión de los derechos de acceso al usuario	SI	
			A.11.3	Responsabilidades del usuario	A.11.3.1	Uso de clave	SI	Así se evitará el acceso de usuarios no autorizados, también se evitará el robo de la información y los medios de procesamiento de la información
					A.11.3.2	Equipo de usuario desatendido	SI	
					A.11.3.3	Política de pantalla y escritorio limpio	SI	
			A.11.6	Control de acceso a la información y aplicación	A.11.6.1	Restricción al acceso a la información	SI	Para evitar el acceso no autorizado a la información mantenida en los sistemas de aplicación

					A.11.6.2	Aislamiento del sistema sensible	SI	
	A.12	Adquisición, desarrollo y mantenimiento de los sistemas de información	A.12.1	Requerimientos de seguridad de los sistemas	A.12.1.1	Análisis y especificación de los requerimientos de seguridad	SI	Asegurar que la seguridad sea una parte integral de los sistemas de información
			A.12.2	Procesamiento correcto en las aplicaciones	A.12.2.1	Validación de la data de insumo	SI	Permite asegurar que la data sea correcta y apropiada
					A.12.2.2	Control de procesamiento interno	SI	Para detectar cualquier corrupción de la información
					A.12.2.3	Integridad del mensaje	SI	Para asegurar la autenticidad y protección de la integridad de mensaje en las aplicaciones
					A.12.2.4	Validación de la data de output	SI	Asegurar que el procesamiento de la información almacenada sea correcto y apropiado para las circunstancias

			A.12.4	Seguridad de los archivos del sistema	A.12.4.1	Control de software operacional	SI	Para garantizar la seguridad de los archivos del sistema
					A.12.4.2	Protección de la data de prueba del sistema	SI	
					A.12.4.3	Control de acceso al código fuente del programa	SI	
			A.12.5	Seguridad de los procesos de desarrollo y soporte	A.12.5.1	Procedimiento de control de cambio	SI	Para mantener la seguridad del software e información del sistema de aplicación
					A.12.5.2	Revisión técnica de las aplicaciones después de cambios en el sistema operativo	SI	
					A.12.5.3	Restricciones sobre los cambios en los paquetes de software	SI	

			A.12.6	Gestión de vulnerabilidad técnica	A.12.6.1	Control de vulnerabilidades técnicas	SI	Para reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas publicadas
Cancelaciones	A.8	Seguridad de los Recursos Humanos	A.8.1	Antes del Empleo	A.8.1.1	Roles y Responsabilidades	SI	Para asegurar que los empleados entiendan sus responsabilidades.
					A.8.1.2	Selección	SI	Para garantizar que los empleados sean los más adecuados para los roles.
					A.8.1.3	Términos y condiciones de empleo	SI	Permitirá reducir los riesgos de robo, fraude o mal uso de los medios.
			A.8.2	Durante el empleo	A.8.2.1	Gestión de responsabilidades	SI	Con el fin de que los empleados estén al tanto de sus responsabilidades y apliquen las políticas de seguridad de la información de la organización.
					A.8.2.2	Capacitación en educación en seguridad de la información	SI	Para asegurar que los empleados estén al tanto de las amenazas e inquietudes sobre la seguridad de la información

					A.8.2.3	Proceso disciplinario	SI	Como apoyo a la concienciación a la seguridad de la información.
			A.8.3	Terminación o cambio de empleo	A.8.3.1	Responsabilidades de terminación	SI	Asegurar que los empleados salgan de la organización de una manera segura.
					A.8.3.2	Devolución de activos	SI	
					A.8.3.3	Eliminación de derechos de acceso	SI	
Libro de rutas	A.6	Organización de la Seguridad de la información	A.6.1	Organización interna	A.6.1.1	Compromiso de la gerencia con la seguridad de la información	SI	Manejar la seguridad de la información dentro de la organización
					A.6.1.2	Coordinación de la seguridad de la información	SI	

					A.6.1.3	Asignación de responsabilidades de la seguridad de la información	SI	
					A.6.1.4	Proceso de autorización para los medios de procesamiento de información	SI	
					A.6.1.5	Acuerdos de confidencialidad	SI	
					A.6.1.6	Contacto con autoridades	SI	
					A.6.1.8	Revisión independiente de la seguridad de la información	SI	
	A.7	Gestión de activos	A.7.1	Responsabilidad por los activos	A.7.1.1	Inventario de activos	SI	Lograr y mantener la protección apropiada de los activos organizacionales

					A.7.1.2	Propiedad de los activos	SI	
					A.7.1.3	Uso aceptable de los activos	SI	
			A.7.2	Clasificación de la información	A.7.2.1	Lineamientos de clasificación	SI	Asegurar que la información reciba un nivel de protección apropiado
					A.7.2.2	Etiquetado y manejo de la información	SI	
	A.8	Seguridad de los Recursos Humanos	A.8.1	Antes del Empleo	A.8.1.1	Roles y Responsabilidades	SI	Para asegurar que los empleados entiendan sus responsabilidades.
					A.8.1.2	Selección	SI	Para garantizar que los empleados sean los más adecuados para los roles.

					A.8.1.3	Términos y condiciones de empleo	SI	Permitirá reducir los riesgos de robo, fraude o mal uso de los medios.
			A.8.2	Durante el empleo	A.8.2.1	Gestión de responsabilidades	SI	Con el fin de que los empleados estén al tanto de sus responsabilidades y apliquen las políticas de seguridad de la información de la organización.
					A.8.2.2	Capacitación en educación en seguridad de la información	SI	Para asegurar que los empleados estén al tanto de las amenazas e inquietudes sobre la seguridad de la información
					A.8.2.3	Proceso disciplinario	SI	Como apoyo a la concienciación a la seguridad de la información.
			A.8.3	Terminación o cambio de empleo	A.8.3.1	Responsabilidades de terminación	SI	Asegurar que los empleados salgan de la organización de una manera segura.
					A.8.3.2	Devolución de activos	SI	

					A.8.3.3	Eliminación de derechos de acceso	SI	
Clientes	A.8	Seguridad de los Recursos Humanos	A.8.1	Antes del Empleo	A.8.1.1	Roles y Responsabilidades	SI	Para asegurar que los empleados entiendan sus responsabilidades.
					A.8.1.2	Selección	SI	Para garantizar que los empleados sean los más adecuados para los roles.
					A.8.1.3	Términos y condiciones de empleo	SI	Permitirá reducir los riesgos de robo, fraude o mal uso de los medios.
			A.8.2	Durante el empleo	A.8.2.1	Gestión de responsabilidades	SI	Con el fin de que los empleados estén al tanto de sus responsabilidades y apliquen las políticas de seguridad de la información de la organización.
					A.8.2.2	Capacitación en educación en seguridad de la información	SI	Para asegurar que los empleados estén al tanto de las amenazas e inquietudes sobre la seguridad de la información

					A.8.2.3	Proceso disciplinario	SI	Como apoyo a la concienciación a la seguridad de la información.
			A.8.3	Terminación o cambio de empleo	A.8.3.1	Responsabilidades de terminación	SI	Asegurar que los empleados salgan de la organización de una manera segura.
					A.8.3.2	Devolución de activos	SI	
					A.8.3.3	Eliminación de derechos de acceso	SI	
Factura	A.8	Seguridad de los Recursos Humanos	A.8.1	Antes del Empleo	A.8.1.1	Roles y Responsabilidades	SI	Para asegurar que los empleados entiendan sus responsabilidades.
					A.8.1.2	Selección	SI	Para garantizar que los empleados sean los más adecuados para los roles.

					A.8.1.3	Términos y condiciones de empleo	SI	Permitirá reducir los riesgos de robo, fraude o mal uso de los medios.
			A.8.2	Durante el empleo	A.8.2.1	Gestión de responsabilidades	SI	Con el fin de que los empleados estén al tanto de sus responsabilidades y apliquen las políticas de seguridad de la información de la organización.
					A.8.2.2	Capacitación en educación en seguridad de la información	SI	Para asegurar que los empleados estén al tanto de las amenazas e inquietudes sobre la seguridad de la información
					A.8.2.3	Proceso disciplinario	SI	Como apoyo a la concienciación a la seguridad de la información.
			A.8.3	Terminación o cambio de empleo	A.8.3.1	Responsabilidades de terminación	SI	Asegurar que los empleados salgan de la organización de una manera segura.
					A.8.3.2	Devolución de activos	SI	

					A.8.3.3	Eliminación de derechos de acceso	SI	

5.7 Aprobación de la Gerencia para los riesgos residuales

(La decisión de la gerencia ha sido registrada en una carta, ver Anexo A4).

5.8 Política de Seguridad – Propuesta

La política se debe basar en el análisis de riesgo y tener como objetivo la estandarización de entornos y procesos de manera que se eviten las vulnerabilidades existentes. Su creación está directamente conectada a la concretización de este análisis, pues a través del levantamiento de las vulnerabilidades se puede elaborar la documentación de seguridad, con el objetivo de minimizar los riesgos de que las amenazas se conviertan en incidentes, de tal forma que se ha planteado la siguiente política de seguridad:

PLAN DE SEGURIDAD DE LA INFORMACIÓN

OBJETIVO GENERAL

Elaborar un Plan de Seguridad de la Información para Orotoni Cía. Ltda., con el fin de establecer una cultura de la seguridad en la organización.

ANTECEDENTES

Como requisito para el establecimiento de un Sistema de Gestión de Seguridad de la Información para Orotoni Cía. Ltda., basado en la norma ISO/IEC 27001:2005.

ALCANCE

El documento de Política de Seguridad de la Información se aplica para todos los empleados de Orotoni Cía. Ltda., así como a las entidades externas que desempeñen labores o le proporcionen algún tipo de servicio o producto.

DESARROLLO

1.- POLITICA DE SEGURIDAD DE LA INFORMACIÓN

1.1 La gerencia debe aprobar un documento de política de seguridad de la información.
1.2 El documento de política de seguridad de la información se debe publicar y comunicar a todos los empleados y entidades externas relevantes.
1.3 La política de seguridad de la información debe ser revisada regularmente a intervalos planeados o si ocurren cambios significativos para asegurar la continua idoneidad, eficiencia y efectividad.

2.- POLITICA DE SEGURIDAD DE LA INFORMACIÓN DENTRO DE LA ORGANIZACIÓN

2.1 La gerencia debe apoyar activamente la seguridad dentro de la organización.
2.2 Las actividades de seguridad de la información deben ser coordinadas por representantes de diferentes partes de la organización con las funciones y roles laborales relevantes.

3.- POLITICAS DE SEGURIDAD DE LA INFORMACIÓN RELACIONADOS CON ENTIDADES EXTERNAS

3.1 Se deben identificar los riegos (relacionados con entidades externas) que corren la información y los medios de procesamiento de la información de la organización.
3.2 Se deben tratar todos los requerimientos de seguridad identificados antes de otorgar a los clientes acceso a la información o activos de la organización.

4.- POLITICAS DE SEGURIDAD AL GESTIONAR ACTIVOS

4.1 Se debe elaborar y mantener un inventario de todos los activos importantes.
4.2 La información y los activos asociados con los medios de procesamiento de la información deben ser responsabilidad de una parte designada de la organización.
4.3 Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con los medios de procesamiento de la información.

4.4 La información debe ser clasificada en términos de su valor, requerimientos legales, confidencialidad y grado crítico para la organización.

5.- POLÍTICAS DE SEGURIDAD DE LOS RECURSOS HUMANOS

5.1 Se deben definir y documentar los roles y responsabilidades de seguridad de los empleados, contratistas y terceros en concordancia con la política de seguridad de la información de la organización.
5.2 Se deben llevar a cabo chequeos de verificación de antecedentes de todos los candidatos a empleados, contratistas y terceros en concordancia con las leyes, regulaciones y ética relevante.
5.3 Los empleados, contratistas y terceros deben aceptar y firmar los términos y condiciones de su contrato de empleo, el cual debe establecer sus responsabilidades y las de la organización para la seguridad de la información.
5.4 Los empleados, contratistas y terceros deben recibir el apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral.
5.5 Debe existir un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad.
5.6 Se deben definir y asignar claramente las responsabilidades para realizar la terminación del empleo.
5.7 Todos los empleados deben devolver todos los activos de la organización que estén en su posesión a la terminación de su empleo.
5.8 Los derechos de acceso (a todos los empleados) a la información y medios de procesamiento de información deben ser eliminados a la terminación de su empleo.

6.- POLITICAS DE SEGURIDAD FÍSICA Y AMBIENTAL

6.1 Se deben utilizar perímetros de seguridad (puertas de ingreso controlado) para proteger áreas que contienen información y medios de procesamiento de información.
6.2 Se debe diseñar y aplicar protección física contra daño por fuego, inundación terremoto, explosión, disturbios civiles y otras formas de desastre natural o creado por el hombre.

6.3 Se deben controlar los puntos de acceso como las áreas de entrega y descarga y otros puntos donde personas no autorizadas pueden ingresar a los locales.
6.4 El equipo debe estar ubicado o protegido para reducir los riesgos de las amenazas y peligros ambientales.
6.5 El equipo debe ser protegido de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos.
6.6 Se debe aplicar seguridad al equipo fuera del local tomando en cuenta los diferentes riesgos de trabajar fuera del local de la organización.
6.7 Los equipos no deben ser sacados fuera de la propiedad sin previa autorización.

7.- POLÍTICAS DE SEGURIDAD DE LA GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES

7.1 Se deben documentar y mantener los procedimientos de operación y se deben poner a disposición de los usuarios que los necesiten.
7.2 Se deben establecer los criterios de aceptación para los sistemas de información nuevos, actualizaciones y versiones nuevas y se deben llevar a cabo pruebas adecuadas del sistema o sistemas durante su desarrollo y antes de su aceptación.
7.3 Se deben implementar controles de detección, prevención y recuperación para protegerse de los códigos maliciosos.
7.4 Se deben realizar copias de backup de la información comercial y software esencial y se deben probar regularmente.
7.5 Las redes deben ser adecuadamente manejadas y controladas para poderlas proteger de amenazas, y para mantener la seguridad de los sistemas y aplicaciones utilizando la red, incluyendo la información de tránsito.
7.6 Deben existir procedimientos para la gestión de medios removibles.
7.7 Se deben establecer acuerdos para el intercambio de información y software entre la organización y las entidades externas.
7.8 Se deben proteger adecuadamente los mensajes electrónicos.
7.9 Se deben producir registros de las actividades de auditoría, excepciones y eventos de seguridad de la información y se deben mantener durante un período acordado para ayudar en investigaciones futuras y monitorear el control de acceso.
7.10 Los relojes de sistemas de procesamiento de información relevantes de una organización o dominio de seguridad deben estar sincronizados con una fuente de tiempo exacta acordada.

8.- POLÍTICAS DE SEGURIDAD DE CONTROL DE ACCESO

8.1 Se debe restringir y controlar la asignación y uso de privilegios de los usuarios.
8.2 La asignación de claves se debe controlar a través de un proceso de gestión formal.
8.3 Se debe requerir que los usuarios sigan buenas prácticas de seguridad en la selección y uso de claves.
8.4 Se debe utilizar métodos de autenticación para controlar el acceso de usuarios remotos.
8.5 Todos los usuarios deben tener un ID de usuario para su uso personal y exclusivo.
8.6 Los sistemas sensibles deben tener un ambiente de cómputo dedicado.

9.- POLÍTICAS DE SEGURIDAD DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

9.1 Los enunciados de los requerimientos comerciales para sistemas nuevos o mejorar los sistemas existentes deben especificar los requerimientos de los controles de seguridad.
9.2 Los datos de entrada deben ser validados para asegurar que esa data sea correcta y apropiada.
9.3 Se deben incorporar chequeos de validación en las aplicaciones para detectar cualquier corrupción de la información a través de errores de procesamiento o actos deliberados.
9.4 Se debe validar el output de data de una aplicación para asegurar que el procesamiento de la información almacenada sea correcto y apropiado para las circunstancias.
9.5 Se debe contar con procedimientos para controlar la instalación de software en los sistemas operacionales.
9.6 Se debe restringir el acceso al código fuente del programa.
9.7 La implementación de cambios se debe controlar mediante el uso de procedimientos formales de control de cambios.
9.8 No se deben fomentar las modificaciones a los paquetes de software, se deben limitar a los cambios necesarios y todos los cambios deben ser controlados estrictamente.
9.9 Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información en uso, se debe evaluar la

exposición de la organización ante esas vulnerabilidades y se deben tomar las medidas apropiadas para tratar el riesgo asociado.

10.- POLÍTICAS DE SEGURIDAD DE GESTIÓN DE INCIDENTES

10.1 Los eventos de seguridad de la información deben reportarse a través de los canales gerenciales apropiados lo más rápidamente posible.
10.2 Se deben establecer las responsabilidades y procedimientos gerenciales para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.

11.- POLÍTICAS DE SEGURIDAD DE LA GESTIÓN DE LA CONTINUIDAD COMERCIAL

11.1 Se deben identificar los eventos que causan interrupciones en los procesos comerciales, junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias para la seguridad de la información.
11.2 Se deben desarrollar e implementar planes para mantener o restaurar las operaciones y asegurar la disponibilidad de la información en el nivel requerido y en las escalas de tiempo requeridas después de la interrupción o fallas en los procesos comerciales críticos.
11.3 Los planes de continuidad comercial se deben probar y actualizar regularmente para asegurar que sean efectivos.

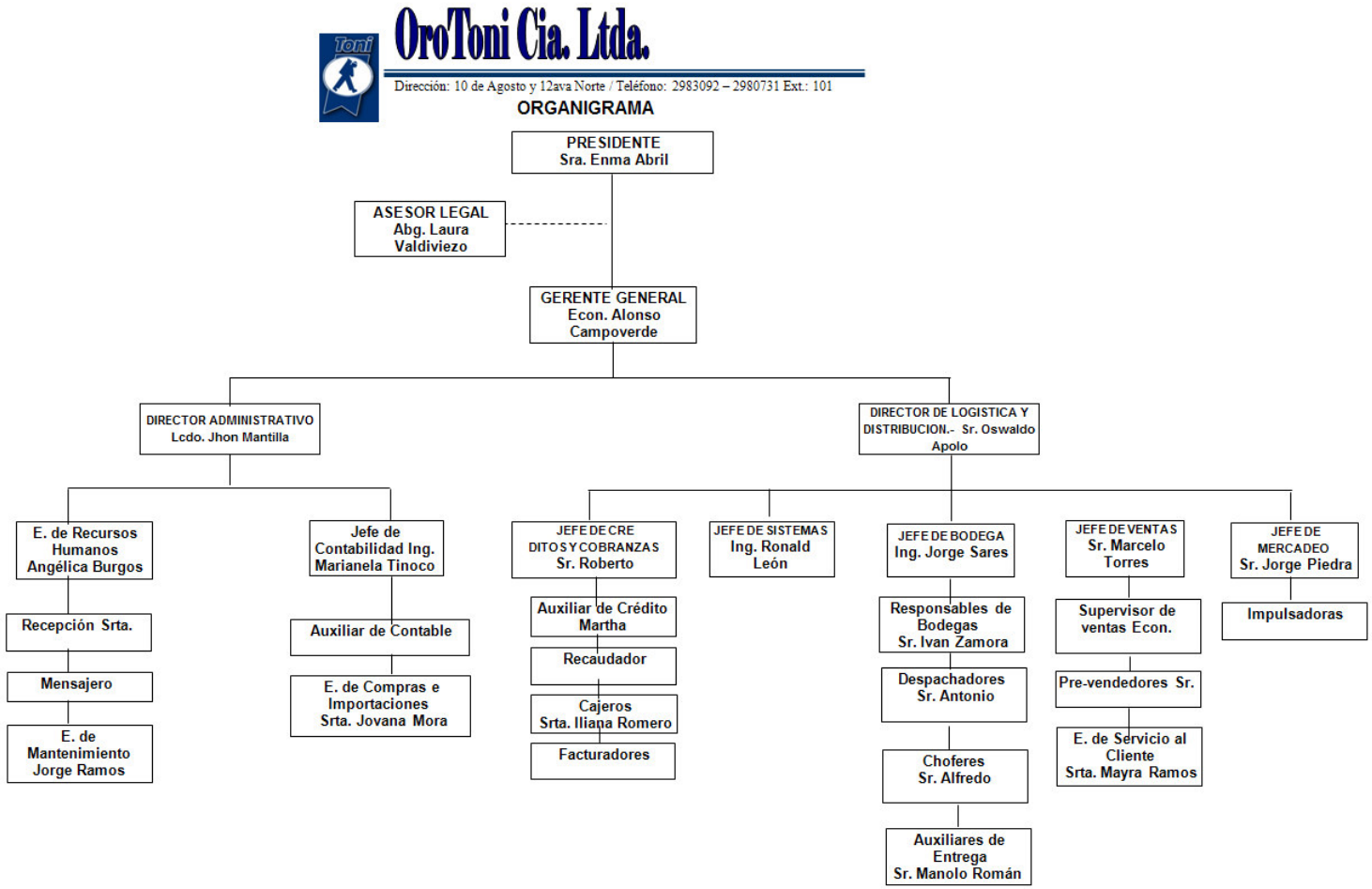
12.- POLÍTICAS DE SEGURIDAD DE CUMPLIMIENTO

12.1 Se deben evitar violaciones de cualquier ley, obligación reguladora o contractual.
12.2 Se debe desanimar a los usuarios de utilizar los medios de procesamiento de la información para propósitos no autorizados.
12.3 Se deben planear cuidadosamente los requerimientos y actividades de las auditorias que involucran chequeos de los sistemas operacionales y se debe acordar minimizar el riesgo de interrupciones en los procesos comerciales.

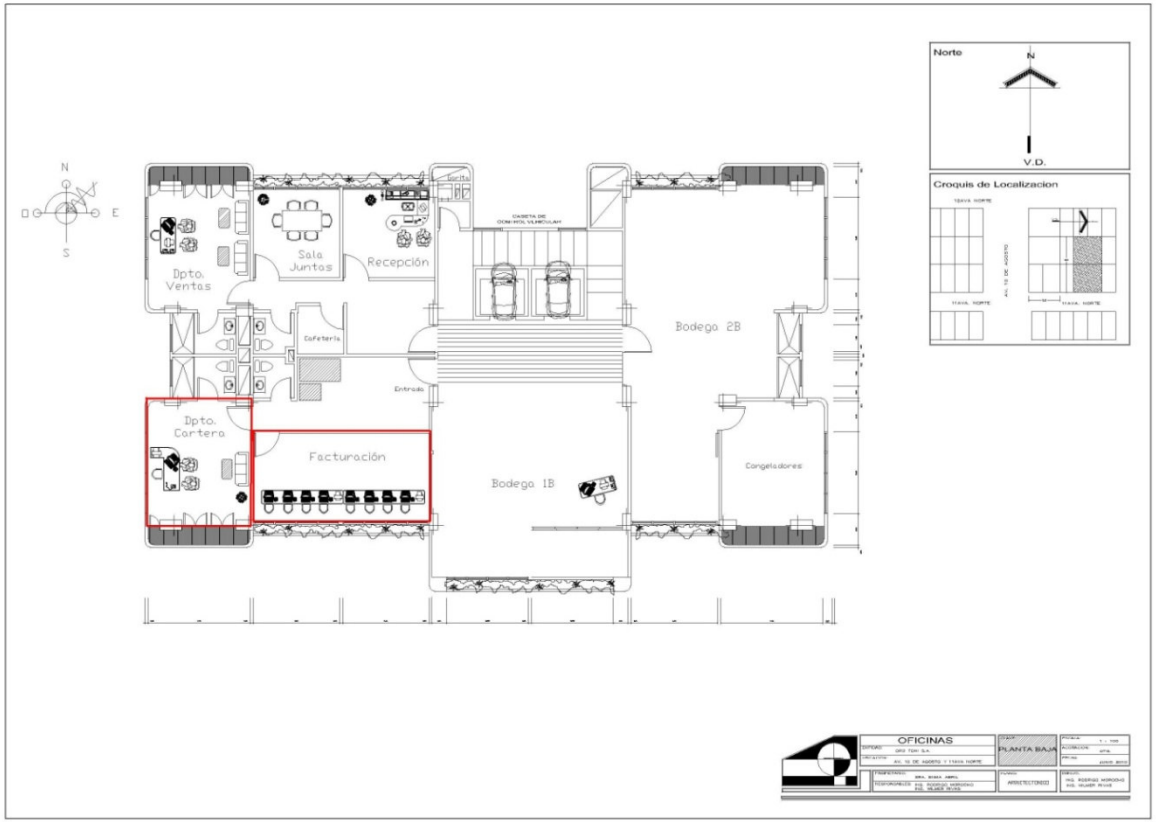
CONCLUSION

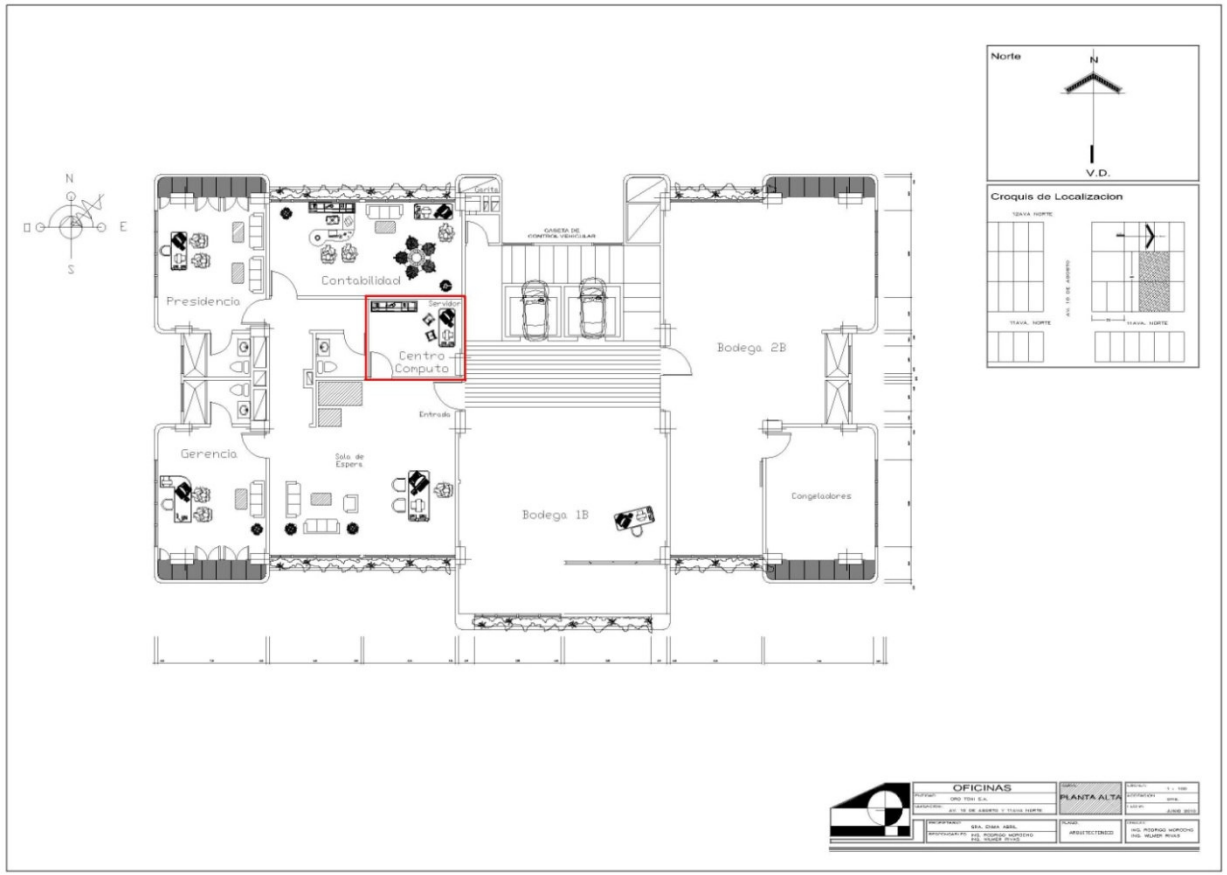
Esperamos que el presente proyecto sirva de ayuda para la Empresa Orotoni Cía. Ltda., para que pueda alcanzar los objetivos de seguridad y mejorar los valores de confidencialidad, integridad y disponibilidad de la información. Que el establecimiento del Sistema de gestión de seguridad sea implementado y sirva para la certificación de la Norma ISO 27001.

ANEXO A1: ORGANIGRAMA



ANEXO A2: DETALLE DE LOS LÍMITES FÍSICOS DEL SGSI




Norte
N
V.D.
Croquis de Localizacion
N
S
E
Presidencia
Contabilidad
Servidor
Centro Computo
Entrada
Gerencia
Sala de Espera
Bodega 2B
Bodega 1B
Congeladores
OFICINAS
PLANTA ALTA
ARQUITECTONICO

ANEXO A3: Carta de procesos considerados y excluidos por parte de la gerencia

OROTONI CIA. LTDA

Dirección: 12va. Norte entre 10 de agosto y vía Limón
Teléfonos: 2980-731 2983-092

Machala, 12 de Marzo de 2010

Señores

Asesores de seguridad

Ciudad.-

De mis consideraciones

En uso de mis atribuciones como Gerente General de OROTONI CIA. LTDA., declaro estar de acuerdo con los procesos que serán considerados para el establecimiento del Sistema de Gestión de Seguridad de la Información según la norma ISO 27001, tomando en cuenta la criticidad de los mismos y por ende su importancia para la organización; a saber:

Proceso estratégico (Mantenimiento de Tablas)

Procesos operativos (Pedidos a Clientes, Facturación, Crédito)

De igual forma declaro estar de acuerdo con los procesos que han sido excluidos, a saber:

Procesos estratégicos (Planificación libro de rutas, Presupuestos, Supervisión de ventas, Marketing, Compras, Gestión con proveedores)

Procesos operativos (Despacho, Entrega)

Procesos de soporte (Gestión de recursos Humanos, Gestión de Sistemas de Información, Gestión de mantenimiento de infraestructura, Gestión administrativa)

Atentamente,

Econ. Alonso Campoverde
Gerente General de Orotoni S.A.

ANEXO A4: Carta de decisión de mitigar el riesgo

OROTONI CIA. LTDA

Dirección: 12va. Norte entre 10 de agosto y vía Limón
Teléfonos: 2980-731 2983-092

Machala, 16 de Abril de 2010

Señores

Asesores de seguridad

Ciudad.-

De mis consideraciones

En uso de mis atribuciones como Gerente General de OROTONI CIA. LTDA., declaro estar de acuerdo con la decisión de Mitigar los Riesgos como forma de administración de los mismos a través del uso de controles según ha quedado establecido y aprobado en el Enunciado de Aplicabilidad presentado a esta gerencia.

Sirva este documento para los fines pertinentes al Establecimiento del SGSI – Sistema de Gestión de Seguridad de la Información para Orotoni Cia. Ltda., según la norma ISO 27001.

Atentamente;

Econ. Alonso Campoverde
Gerente General de Orotoni

ANEXO A5: FUENTE DE CALIFICACIÓN – TASACIÓN DE ACTIVOS Y PRIORIZACIÓN DEL RIESGO

Se creó un comité conformado por el Presidente (Sra. Enma Abril), Gerente General (Econ. Alonso Campoverde), Jefe de Ventas (Sr. Marcelo Torres), esto con el objetivo de establecer la tasación de activos y evaluación de los riesgos de los procesos considerados como críticos.

Para llevar a cabo esta labor, se capacitó en cuanto a los conceptos de disponibilidad, integridad y confidencialidad de la información y los activos relacionados, lo mismo respecto de amenazas y vulnerabilidades.

Luego del trabajo en grupo y deliberación, se obtuvo una puntuación, para situar la gravedad del impacto, generando las tablas detalladas en los puntos 4.4.2 Tasación de activos y 4.5 Análisis y Evaluación del Riesgo.

ANEXO A6: GLOSARIO

Backup

Una copia de seguridad o backup es un archivo digital, un conjunto de archivos o la totalidad de los datos considerados lo suficientemente importantes para ser conservados, Fundamentalmente son útiles para poder recuperarse de una catástrofe informática o para recuperar una pequeña cantidad de archivos que pueden haberse eliminado accidentalmente o corrompido.

Basilea II

Segundo de los Acuerdos de Basilea. Dichos acuerdos consisten en recomendaciones sobre la legislación y regulación bancaria y son emitidos por el Comité de supervisión bancaria de Basilea. El propósito de Basilea II, publicado inicialmente en junio de 2004, es la creación de un estándar internacional que sirva de referencia a los reguladores bancarios, con objeto de establecer los requerimientos de capital necesarios, para asegurar la protección de las entidades frente a los riesgos financieros y operativos.

Chief Information Security Officer (CISO)

Ejecutivo de alto nivel dentro de una organización, responsable de establecer y mantener la visión empresarial, la estrategia y programa para garantizar los activos de información están adecuadamente protegidos.

Ciberataques

Son actos en los cuales se cometen agravios, daños o perjuicios en contra de las personas o grupos de ellas, entidades o instituciones y que por lo general son ejecutados por medio de computadoras y a través de la Internet. No necesariamente pueden ser cometidos totalmente por estos medios, sino también a partir de los mismos. Un ciberataque puede estar dirigido a los equipos y sistemas de computación que se encuentran operando en la red a nivel mundial, o puede ser orientado hacia la información y los datos que son almacenados en bases de datos. Al dirigirse a los equipos y sistemas, pueden buscar la anulación del servicio que éstos prestan, en forma temporal o permanente, introduciendo algún tipo de elementos extraños en dichos sistemas que dificulten su operación normal. Los ataques contra los datos, por su parte, pueden ir desde el robo de los mismos con propósitos militares o comerciales.

Cifrado

Es el proceso para volver ilegible información considera importante. La información una vez encriptada sólo puede leerse aplicándole una clave.

Se trata de una medida de seguridad que es usada para almacenar o transferir información delicada que no debería ser accesible a terceros. Pueden ser contraseñas, números de tarjetas de crédito, conversaciones privadas, etc.

Para cifrar o encriptar información se utilizan complejas fórmulas matemáticas y para desencriptar, se debe usar una clave como parámetro para esas fórmulas.

Cobit (Objetivos de Control para la Información y las Tecnologías relacionadas)

El estándar Cobit (Control Objectives for Information and related Technology) ofrece un conjunto de "mejores prácticas" para la gestión de los Sistemas de Información de las organizaciones.

El objetivo principal de Cobit consiste en proporcionar una guía a alto nivel sobre puntos en los que establecer controles internos con tal de:

- Asegurar el buen gobierno, protegiendo los intereses de los stakeholders (clientes, accionistas, empleados, etc.)
- Garantizar el cumplimiento normativo del sector al que pertenezca la organización
- Mejorar la eficacia y eficiencia de los procesos y actividades de la organización
- Garantizar la confidencialidad, integridad y disponibilidad de la información

El estándar define el término control como: "Políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para proveer aseguramiento razonable de que se lograrán los objetivos del negocio y se prevendrán, detectarán y corregirán los eventos no deseables"

Firewall

Herramienta de seguridad que controla el tráfico de entrada/salida de una red.

Estos programas suelen usarse para la protección de una computadora que está conectada a una red, especialmente internet. Controlan todo el tráfico de entrada y de salida, informando o evitando actividades sospechosas. Algunos cortafuegos tienen capacidad de detectar espías y pop-ups. De hecho, muchos antivirus tienen incorporada una herramienta tipo cortafuego.

Firmas digitales

Las firmas digitales son análogas a las firmas manuscritas. Una firma digital es una precisa forma matemática de adjuntar la identidad de una persona a un

mensaje. Son mucho más difíciles de falsificar que las firmas escritas, y el mensaje firmado no puede ser modificado sin invalidar la firma.

Guías ENISA (European Network and Information Security Agency)

Guías de buenas prácticas que contribuyen con la estrategia de la Comisión Europea (UE) sobre Protección de la Infraestructura de Información Crítica.

Ingenieria Social

Práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica que pueden usar ciertas personas, tales como investigadores privados, criminales, o delincuentes computacionales, para obtener información, acceso o privilegios en sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgo o abusos.

Insiders – Atacantes internos

Usuarios de TI internos a la organización. Se refiere a las amenazas a equipos que vienen de parte de personas que han trabajado o trabajan con los mismos.

IPSec (Internet Protocol Security)

Es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando o cifrando cada paquete IP en un flujo de datos.

ISM3 (Information Security Management Maturity Model)

Nuevo estándar para la gestión de la seguridad de la información, (conocido como ISM-cubed o ISM3) está construido en estándares como: ITIL, ISO 20000, ISO 9001, CMM, ISO/IEC 27001, e información general de conceptos de seguridad de los gobiernos. Mientras que la ISO/IEC 27001 está basada en controles. ISM3 está basada en procesos e incluye métricas de proceso.

ISM3 pretende cubrir la necesidad de un estándar simple y aplicable de calidad para sistemas de gestión de la seguridad de la información, proporciona un marco para ISM que puede utilizarse tanto por pequeñas organizaciones que realizan sus primeros esfuerzos, como a un nivel alto de sofisticación por grandes organizaciones como parte de sus procesos de seguridad de la información.

ITIL (Information Technology Infrastructure Library)

La Biblioteca de Infraestructura de Tecnologías de Información, frecuentemente abreviada ITIL, es un marco de trabajo de las buenas prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información (TI). ITIL resume

un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI. Estos procedimientos son independientes del proveedor y han sido desarrollados para servir como guía que abarque toda infraestructura, desarrollo y operaciones de TI.

Magerit (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información)

MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.

La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza.

Malware

Malware (del inglés malicious software), también llamado badware, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario. El término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto.

NIST (National Institute of Standards and Technology)

El Instituto Nacional de Normas y Tecnología, es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos. La misión de este instituto es promover la innovación y la competencia industrial en Estados Unidos mediante avances en metrología, normas y tecnología de forma que mejoren la estabilidad económica y la calidad de vida.

Como parte de esta misión, los científicos e ingenieros del NIST continuamente refinan la ciencia de la medición (metrología) creando una ingeniería precisa y una manufacturación requerida para la mayoría de los avances tecnológicos actuales. También están directamente involucrados en el desarrollo y pruebas de normas hechos por el sector privado y agencias de gobierno. El NIST fue originalmente llamado Oficina Nacional de Normas (NBS por sus siglas en inglés), un nombre que tuvo desde 1901 hasta 1988. El progreso e innovación tecnológica de Estados Unidos dependen de las habilidades del NIST, especialmente si hablamos de cuatro áreas: biotecnología, nanotecnología, tecnologías de la información y fabricación avanzada.

Octave (Operationally Critical Threat, Asset, and Vulnerability Evaluation)

Es un marco para identificar y gestionar los riesgos de seguridad de información. Se define un método de evaluación integral que permite a una organización identificar los activos de información que son importantes para la misión de la organización, las amenazas a esos bienes, y las vulnerabilidades que pueden exponer a los activos a las amenazas. Al juntar los activos de información, las amenazas y vulnerabilidades, la organización puede comenzar a entender qué información está en riesgo. Con este entendimiento, la organización puede diseñar e implementar una estrategia de protección para reducir la exposición global al riesgo de sus activos de información.

OSSTM (Open Source Security Testing Methodology **Manual)**

El "Manual de la Metodología Abierta de Testeo de Seguridad" es un documento que reúne, de forma estandarizada y ordenada, las diversas verificaciones y pruebas que debe realizar un profesional de la seguridad informática durante el desarrollo de las auditorías y verificaciones de la seguridad. Es un documento en constante evolución, fruto del trabajo conjunto de más de 150 colaboradores de todo el mundo.

La participación directa de estos profesionales, que desarrollan su actividad profesional en el sector de la seguridad, en la confección de la metodología le permite incorporar los más recientes cambios y nuevas tendencias en el mundo de la seguridad informática.

Outsoursing

La subcontratación (outsourcing, por su término en inglés) es el proceso económico en el cual una empresa determinada mueve o destina los recursos orientados a cumplir ciertas tareas, a una empresa externa, por medio de un contrato. Esto se da especialmente en el caso de la subcontratación de empresas especializadas.

Pharming

Es la explotación de una vulnerabilidad en el software de los servidores DNS (Domain Name System) o en el de los equipos de los propios usuarios, que permite a un atacante redirigir un nombre de dominio (domain name) a otra máquina distinta. De esta forma, un usuario que introduzca un determinado nombre de dominio que haya sido redirigido, accederá en su explorador de internet a la página web que el atacante haya especificado para ese nombre de dominio.

Phishing

Es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria).

Sarbanes Oxley (SOX)

Es una ley que nace en Estados Unidos con el fin de monitorear a las empresas que cotizan en bolsa, evitando que las acciones de las mismas sean alteradas de manera dudosa, mientras que su valor es menor. Su finalidad es evitar fraudes y riesgo de bancarrota, protegiendo al inversor.

Sistemas de detección de intrusos

Un sistema de detección de intrusos (IDS - Intrusion Detection System) es un programa usado para detectar accesos no autorizados a un computador o a una red. Estos accesos pueden ser ataques de habilidosos hackers que usan herramientas automáticas.

Sistemas Biométricos

Se refiere a las tecnologías para medir y analizar las características físicas y del comportamiento humanas con propósito de autentificación.

Software Development LifeCycle (SDLC)

Metodología para el desarrollo de un producto de software. Términos similares incluyen el ciclo de vida del software y procesos de software.

BIBLIOGRAFÍA

Estándares:

- Norma ISO/IEC 27001:2005, Tecnología de Información-Técnicas de Seguridad-Sistemas de Gestión de Seguridad de la Información-Requerimientos
- Norma ISO/IEC 17799:2005, Tecnología de Información-Técnicas de Seguridad-Código de práctica para la gestión de la seguridad de la información

Sitios web:

- http://www.segu-info.com.ar(http://www.segu-info.com.ar/articulos/93-informes-estudios-seguridad-informacion.htm)
- http://www.iso27000.es/sgsi.html

Otros documentos:

Informe - Seguridad de la Información en Latinoamérica, Tendencias 2009, Jeimy J. Cano, Ph.D, Coordinador Segurinfo