|  |
| --- |
| Diseño de plan de seguridad de datos para una institución basado en ISO27k |
|  |
| 10 abril  PANADERIA DIANA  Creado por: Reinaldo Antonio Chica   Anderson Emmanuel Morales Lazo  Carlos Manuel Ramirez Rubio  Edin Ivan Saravia Vigil  Joel Cristopher Turcios Turcios |

**Índice**

[*1* capítulo 1 3](#_Toc100496978)

[*1.1* Introducción: 3](#_Toc100496979)

[*1.2* Objetivos 4](#_Toc100496980)

[*1.3* Cronograma de activades 5](#_Toc100496981)

[*2* capitulo 2 6](#_Toc100496982)

[*2.1* Situación actual. 6](#_Toc100496983)

[*2.1.1* Descripción de la organización. 7](#_Toc100496984)

[*2.1.2* Actividad y Entorno 7](#_Toc100496985)

[*2.1.3* Estructura organizacional 8](#_Toc100496986)

[*2.2* Análisis de riesgo. 10](#_Toc100496987)

[*2.2.1* Identificación de activos. 11](#_Toc100496988)

[*2.2.2* Identificación de amenazas y vulnerabilidades 15](#_Toc100496989)

[*2.2.3* Cálculo de la probabilidad 18](#_Toc100496990)

[*2.2.4* Evaluación del riesgo 19](#_Toc100496991)

# *1* capítulo 1

## ***1.1* Introducción:**

Muchas empresas se enfocan más en su actividad comercial y en su productividad, dejando a un lado aspectos tan importantes como los de establecer y fortalecer los controles sobre la seguridad de la información y sus datos para prevenir y detectar fraudes en la compañía. Se confían al no creer ser víctimas de ataques y no se preparan para enfrentar si llegara a suceder.

La seguridad de la información no solo es responsabilidad del departamento de tecnología, sino toda la empresa, por eso es importante concientizar a todo el personal sobre las amenazas y las consecuencias que estas generan.

He aquí el grado de importancia de seguir un modelo de seguridad que garantice el manejo adecuado de la información y aseguren los activos vitales a través de normatividades o políticas que regulen las actividades diarias de la empresa. Las cuales deben ser conocidas por todos los empleados a través de capacitaciones, para que se comprometan a hacer buen uso de la información y de los recursos, y finalmente entre todos mantener los principios como la integridad, autenticidad y confidencialidad de la información.

Con la aplicación de este proyecto, se pretende ofrecer a dicha empresa una propuesta de un Sistema de Gestión de Seguridad de la información que permitan implementar lineamientos que conlleven a asegurar la información y los demás activos informáticos, utilizando como marco de referencia de la norma ISO 27001, la cual emplea las mejores prácticas para cumplir los objetivos del proyecto.

## ***1.2* Objetivos**

Objetivo General:

* Desarrollar un plan que permita aplicar las normas ISO27k1 en dicha organización para la confidencialidad de los datos.
* Diseñar y estructurar un Sistema de Gestión de la Seguridad con el fin de promover, mantener y mejorar las condiciones del manejo de la base de datos.
* mantener la Integridad, Disponibilidad, Privacidad, Control y Autenticidad de la información manejada
* Presentar el Plan de Seguridad y Privacidad de la Información, el cual es el documento que dirige la implementación de normas de seguridad según el modelo de las ISO27K1-2

Objetivo Especifico:

* Desarrollar un cronograma que me permita visualizar las actividades programadas para la elaboración de este proyecto.
* Identificar activos de la organización.
* Comunicar e implementar la estrategia de seguridad de la información.
* Realizar análisis de amenazas y vulnerabilidades
* Analizar nivel de riesgos por medio de los activos de la organización.
* Implementar y apropiar el Modelo de Seguridad y Privacidad de la Información
* Programar diferentes reuniones con los miembros de la empresa para recaudar información para este proyecto.
* Hacer uso eficiente y seguro de los recursos de TI.

## ***1.3* Cronograma de activades**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Cronograma | | | | | | | |
| Actividades | 21-marzo | 28-marzo | 4-abril | 11-abril | 18-abril | 25-abril | 2-mayo |
| Introducción | *X* |  |  |  |  |  |  |
| Objetivos | *X* |  |  |  |  |  |  |
| Identificación de la empresa | *X* |  |  |  |  |  |  |
| Planificación | *X* |  |  |  |  |  |  |
| Reuniones con los miembros de la empresa | *x* | *X* |  |  | *x* |  |  |
| Situación actual y descripción de la organización |  | *X* |  |  |  |  |  |
| Actividad y Entorno |  | *X* |  |  |  |  |  |
| Análisis de riesgo e Identificación de activos |  | *X* |  |  |  |  |  |
| Identificación de amenazas y vulnerabilidades, Cálculo de la probabilidad |  |  | *X* |  |  |  |  |
| Evaluación del riesgo, Cálculo del riesgo residual |  |  | *x* | *x* | *X* |  |  |
| Implantación del proyecto |  |  |  |  | *X* |  |  |
| Entrega del proyecto |  |  |  |  | *X* |  |  |

# *2* capitulo 2

## ***2.1* Situación actual.**

PANADERIA DIANA

La organización contribuye a ordenar los medios para que los recursos humanos trabajen en forma unida y efectiva en el logro de los objetivos generales y específicos de la empresa, conlleva una estructura o marco que integra las diversas funciones de la empresa, de acuerdo con un modelo que sugiere por den, arreglo y relación armónica. La planeación y la organización son funciones mediante las que no se logra materialmente el objetivo; pero ordenan los esfuerzos y formulan la estructura adecuada y la posición relativas a las actividades que la empresa habrá de desarrollar. La organización relaciona entre sí las actividades necesarias y asigna responsabilidades a quienes deben desempeñarlas, las actividades básicas relativas a la función de organización hijo: Asignación de recursos (humanos, financieros, materiales), actividades (cómo),responsables (quién), tiempos (cuándo), determinación de grados de especialización y división del trabajo (comercialización, producción, compras, personal), establecimiento de jerarquías (relaciones de autoridad y responsabilidad), designar funciones, determinación de tramos de control, diseño de la estructura organizacional, elaboración de manuales de organización, políticas y procedimientos, entre otros

Las actividades que se deben llevar a cabo en una empresa resultante de suma importancia, pues de ellas depende el alcance de los objetivos. La organización se refiere a la forma en la que se estructuran dichas actividades conforme a las condiciones de la empresa y los recursos para alcanzar los objetivos planteados.

En la Panificadora Diana la organización es informal, derivada de que no eran considerados aspectos como la capacitación de su personal en la elaboración de nuevos productos, identificación de una zona donde no hubiera una panadería y existiera una necesidad no atendida, no se garantiza y asegura la calidad de los insumos y productos a través de buenas prácticas de Manufactura., No se considera la creación de un producto diferenciado y definición de líneas de autoridad.

### *2.1.1* Descripción de la organización.

***2.1.2* Actividad y Entorno**

Diagrama

Descripción generada automáticamente

Este tipo de estructura preséntalas siguientes ventajas y desventajas:

|  |  |
| --- | --- |
| Ventajas | Desventajas |
| * Es sencilla y clara * Se establece una disciplina laboral * Se facilita la rapidez de acción * No hay conflicto de autoridad ni fuga de responsabilidad * Es más fácil y útil en la microempresa | -Se carece de especialización  -Es poco flexible para futuras expansiones  -Es difícil capacitar a un jefe en todos los aspectos que debe coordinar  - Los jefes siempre están saturados y al perderse una de estas se producen trastornos administrativos |

### *2.1.3* Estructura organizacional

Los organigramas propuestos son de tipo Funcional, se basan en la naturaleza de las actividades a realizar y se organizan específicamente por departamentos o secciones, de acuerdo con los principios de la división del trabajo de las labores de una empresa, y aprovecha la preparación y las aptitudes profesionales del personal en donde pueden lograr mayor rendimiento. Esta organización funcional se aplica particularmente en pequeñas, medianas y grandes empresas, donde al frente de cada departamento está un jefe que tiene su cargo una función determinada y como superior de todos los jefes está un director o gerente que coordina las tareas de aquellos que conforman la concepción y propósitos de la empresa.

Actividades que se realizan en la Panadería Diana.

Nuestra Panadería Diana es una empresa que nace con la misión de servir con los alimentos. Es el resultado de tres generaciones dedicadas a hacer un pan de calidad adaptado a las necesidades de nuestros clientes. Somos amantes del buen pan y de los alimentos elaborados con paciencia y buen hacer.

Nuestra Panadería Diana está situada en la ciudad de San Miguel, y pretende ser un referente de la panadería artesanal, y al mismo tiempo un lugar donde nuestros clientes puedan degustar nuestros productos en un entorno agradable y acogedor.

RECIBIR

Recibimos el producto terminado, primeramente, se descarga. Luego, verifica la calidad (aleatoriamente). Se compara la cantidad del pan pedido y recibido, comparar las facturas para tener en cuenta que las fechas son las correctas. Todo esto debe realizarse de manera eficiente y rápida al momento de llegada, en la medida que sea posible.

DESPACHAR

En esta parte empezamos a organizar los pedidos en orden cronológico donde la prioridad será por la fecha de entrega, igualmente lo haremos con la mercancía donde los panes, serán ubicados de acuerdo con las fechas como lo indican los pedidos, es decir, ubicar cerca de la salida los pedidos a salir. Armar de manera correcta cada pedido para darle salida.

## ***2.2* Análisis de riesgo.**

Tabla

Descripción generada automáticamente

### *2.2.1* Identificación de activos.

Una de las primeras actividades a realizar en la implementación de la norma ISO 27001 en una organización es elaborar un inventario de activos que recoja cuáles son los principales activos de información en la organización.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Activos de Información** | | | | |
| Nombre | Descripción | Responsable | Responsabilidad | Observación |
| Base de datos, Copias de seguridad, Claves | Datos Digitales | Tec. Martín Elías de los Ríos Acosta | -Identificar los activos de Información.  -Definir uso aceptable de los activos de  información. | En esta actividad se establece con los colaboradores designados de los Procesos la  inclusión de los activos en la Matriz de inventarios de activos, clasificación y  publicación de la información |
| Correo, Fax, Celulares, Libros | Activos Tangibles | Sara Teresa Sánchez del Pinar | -Hacer mantenimiento periódico y  evaluar clasificación y valoración de  los activos de información. | El responsable de datos personales es una persona física o jurídica, o bien una autoridad pública. También puede serlo un servicio u otro organismo que ya sea solo, o junto con alguno de los anteriores que te hemos mencionado |
| Patentes, Conocimiento, Relaciones | Activos Intangibles | Todos | Reportar cualquier evento que atente  contra la seguridad de la información. | Sin Observación |
| Software | Activos Intangibles | Tec. Martín Elías de los Ríos Acosta | No contiene datos | Sistema Operativo Windows |
| Sistemas Operativos | Activos Intangibles | Tec. Martín Elías de los Ríos Acosta | Buen cumplimiento de sus funciones, estas se basan en la mejora de programas operativos | Sistema Operativo Confiable |
| Activos Físicos | | | | |
| Código | Nombre | Descripción | Propietario | Observación |
| 992, 04-05, 01-02-03-06 | Edificios, Oficinas, Armarios | Infraestructura TI | Jefe Inmediato:  Kenia Jasmín Cruz Rodríguez | Todo en buen estado, con ambiente aceptable |
| 011101 | Estaciones de trabajo, Portátiles | Hardware de TI. | Jefe Inmediato:  Kenia Jasmín Cruz Rodríguez | Una estación de trabajo cuenta, con una silla, archivero, bote de basura lámparas, libreros. |
| E0-E7 | Aire Acondicionado, Alarmas | Controles del Entorno de TI | Jefe Inmediato:  Kenia Jasmín Cruz Rodríguez | Equipos en buen estado. |
| **Activos de Servicios TI** | | | | |
| Nombre | Descripción | Procedimiento | Custodio | Observación |
| Servicios de Autentificación | Mecanismo que identifica a un usuario o un servicio según los criterios predefinidos | Entre las medidas de seguridad implementadas por diferentes compañías en los últimos años, encontramos las técnicas de autenticación en dos pasos | Identifica al área,  dependencia o grupo que  custodia la información.  -Dos Personas | Proceso de autentificación estándar |
| Servicios de red | No contiene datos | El usuario se autentica ante el servidor proporcionando un sujeto principal y una contraseña cuando inicia sesión | Sin Datos | Sin observación |
| **Activos Humanos** | | | | |
| Nombre | Responsabilidad o Rol | Descripción | Idioma | Cantidad de Personas |
| Jefe Inmediato | -Garantizar la confidencialidad,  integridad y disponibilidad del activo  de información. | La Persona a cargo, garantiza el buen desempeño de sus empleados | Español | 1 |
| Empleados | Hacer buen uso de los activos de  información asignados. | Atienden a las normativas y políticas de la organización | Español | 15 |
| Clientes |  | Usuarios | Español | Cantidad Variable, 12 a 25 por día |

Notas:

Estaciones de trabajo: Normalmente, hay estaciones de trabajo individuales y estaciones de trabajo colaborativas.

Formato: identifica la forma, tamaño o modo en la que se presenta la información o se permite su visualización o consulta, se trate de activos de información consistentes en información física o información digital

* Texto (incluye extensiones como .doc, .txt, .rtf, .pdf)
* Hoja de cálculo (incluye extensiones como .xls, .xlt, .csv)
* Presentación (incluye extensiones como .ppt, .pps)
* Documento gráfico (incluye extensiones como .jpg, .gif, .png, .tif, .tiff, .ttf)
* Base de datos (incluye extensiones como .mdb, .sql)
* Compresión (incluye extensiones como .zip, .rar)
* Web (incluye extensiones como .html, .htmls)
* Correo electrónico
* Mensajería instantánea

### *2.2.2* Identificación de amenazas y vulnerabilidades

* **Activos de Información**

|  |  |  |
| --- | --- | --- |
| Activos | Amenazas | Vulnerabilidades |
| Base de datos | Gestión de permisos inadecuada | Preferencia de privilegios de usuario por privilegios de grupo |
| Abuso de Privilegios |
| Ataques de inyección de base de datos | Inyección por SQL |
| Existencia de servidores de bases de datos ocultos | El no tener control de acceso y gestión de derechos |
| Sistema | Fallos de programación | Errores de configuración. |
| Errores en la gestión de recursos |
| Intrusos | Errores en los sistemas de validación |
| Errores que permiten el acceso a directorios |
| Correo Electrónico | Malware | Correo no deseado |
| Extracción de datos |

* **Activos físicos**

|  |  |  |
| --- | --- | --- |
| Activos | Amenazas | Vulnerabilidades |
| Edificios, Oficinas | Destrucción | Bases de construcción débiles |
| Tiempo en la que fue fundado |
| Impuestos | Falta de recursos |
| Pagos de multas |
| Estaciones de trabajo | Perdida de información | Los Servidores no están en un espacio físico adecuado |
| Sistema eléctrico débil por la zona donde se encuentra la estación de trabajo. |
| Mal desempeño del trabajo | Ambiente no apto para trabajar |
| Colocar datos erróneos, debido al estrés que genera el ambiente laboral |
| Aire Acondicionado | Daños a la Salud del personal | Resequedad de las mucosas nasales y esto puede ocasionar molestias |
| Causar desde irritaciones menores a faringitis en personas vulnerables |

* **Activos de Servicios TI**

|  |  |  |
| --- | --- | --- |
| Activos | Amenazas | Vulnerabilidades |
| Servicios de Autentificación | Virus | Sitios web no bloqueos |
| Falta de un antivirus |
| Gusanos | No requieren de la intervención del usuario ni de la modificación de algún archivo para poder infectar un equipo |
| Fallos en el proceso de autentificación de doble factor |
| Servicios de red | Ataques con comandos ping | Denegación de servicio distribuido |
| Session Hijacking o Robos de sesión |

* **Activos Humanos**

|  |  |  |
| --- | --- | --- |
| Activos | Amenazas | Vulnerabilidades |
| Jefe Inmediato | Problemas de Salud | Datos expuestos a terceros |
| Falta de supervisión |
| Empleados | Despidos | Actualización de datos, tardías |
| Datos expuestos a terceros |
| Clientes | Cambios de información frecuentes | Saturación del sistema |
| No aceptar la política de privacidad de la organización | Campos de datos obligatorios |

### *2.2.3* Cálculo de la probabilidad

Nota: Valoración del impacto

* 1 = Bajo
* 2= Medio
* 3= Alto
* **Activos de Información**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Activo** | **Integridad** | **Disponibilidad** | **Confidencialidad** | **Impacto** |
| Base de datos | 2 | 2 | 1 | 2 |
| Sistema | 2 | 2 | 1 | 2 |
| Correo Electrónico | 1 | 2 | 1 | 1 |

* **Activos físicos**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Activo** | **Integridad** | **Disponibilidad** | **Confidencialidad** | **Impacto** |
| Edificios, Oficinas | 2 | 2 | 2 | 2 |
| Estaciones de trabajo | 2 | 1 | 1 | 1 |
| Aire Acondicionado | 1 | 2 | 3 | 3 |

* **Activos de Servicios TI**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Activo** | **Integridad** | **Disponibilidad** | **Confidencialidad** | **Impacto** |
| Servicios de Autentificación | 2 | 1 | 1 | 1 |
| Servicios de red | 1 | 1 | 1 | 1 |

* **Activos Humanos**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Activo** | **Integridad** | **Disponibilidad** | **Confidencialidad** | **Impacto** |
| Jefe Inmediato | 2 | 1 | 1 | 1 |
| Empleados | 2 | 2 | 3 | 2 |
| Clientes | 2 | 2 | 2 | 2 |

### *2.2.4* Evaluación del riesgo

Nota:

* 1= Improbable: Ocurrencia en circunstancias excepcionales, ha ocurrido una vez en 10 años o 20 años
* 2= Probable: Podría ocurrir en algún momento, Ha ocurrido una vez en 2 años o 5 años
* 3= Frecuente: Ocurre en la mayoría de las circunstancias, ha ocurrido una vez en el último año o 6 meses.
* **Activos de Información**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Activos** | **Impacto** | **Amenazas** | **Vulnerabilidades** | **Probabilidad de Ocurrencia** | **Riesgo bruto** |
| Base de datos | 2 | Gestión de permisos inadecuada | Preferencia de privilegios de usuario por privilegios de grupo | 2 | 4 |
| Ataques de inyección de base de datos | Inyección por SQL | 1 | 2 |
| Existencia de servidores de bases de datos ocultos | El no tener control de acceso y gestión de derechos | 2 | 4 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Activos** | **Impacto** | **Amenazas** | **Vulnerabilidades** | **Probabilidad de Ocurrencia** | **Riesgo bruto** |
| Sistema | 2 | Fallos de programación | Errores de configuración | 2 | 4 |
| Errores en la gestión de recursos | 1 | 2 |
| Intrusos | Errores en los sistemas de validación | 2 | 4 |
| Errores que permiten el acceso a directorios | 2 | 4 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Activos** | **Impacto** | **Amenazas** | **Vulnerabilidades** | **Probabilidad de Ocurrencia** | **Riesgo bruto** |
| Correo Electrónico | 1 | Malware | Correo no deseado | 3 | 3 |
| Extracción de datos | 1 | 1 |

* **Activos físicos**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Activos** | **Impacto** | **Amenazas** | **Vulnerabilidades** | **Probabilidad de Ocurrencia** | **Riesgo bruto** |
| Edificios, Oficinas | 2 | Destrucción | Bases de construcción débiles | 1 | 2 |
| Tiempo en la que fue fundado | 1 | 2 |
| Impuestos | Falta de recursos | 2 | 4 |
| Pagos de multas | 2 | 4 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Activos** | **Impacto** | **Amenazas** | **Vulnerabilidades** | **Probabilidad de Ocurrencia** | **Riesgo bruto** |
| Estaciones de trabajo | 1 | Perdida de información | Los Servidores no están en un espacio físico adecuado | 2 | 2 |
| Sistema eléctrico débil por la zona donde se encuentra la estación de trabajo. | 2 | 2 |
| Mal desempeño del trabajo | Ambiente no apto para trabajar | 3 | 3 |
| Colocar datos erróneos, debido al estrés que genera el ambiente laboral | 1 | 1 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Activos** | **Impacto** | **Amenazas** | **Vulnerabilidades** | **Probabilidad de Ocurrencia** | **Riesgo bruto** |
| Aire Acondicionado | 3 | Daños a la Salud del personal | Resequedad de las mucosas nasales y esto puede ocasionar molestias | 2 | 6 |
| Causar desde irritaciones menores a faringitis en personas vulnerables | 1 | 3 |

* **Activos de Servicios TI**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Activos** | **Impacto** | **Amenazas** | **Vulnerabilidades** | **Probabilidad de Ocurrencia** | **Riesgo bruto** |
| Servicios de Autentificación | 1 | Virus | Sitios web no bloqueos | 3 | 3 |
| Falta de un antivirus | 2 | 2 |
| Gusanos | No requieren de la intervención del usuario ni de la modificación de algún archivo para poder infectar un equipo | 2 | 2 |
| Fallos en el proceso de autentificación de doble factor | 1 | 1 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Activos** | **Impacto** | **Amenazas** | **Vulnerabilidades** | **Probabilidad de Ocurrencia** | **Riesgo bruto** |
| Servicios de red | 1 | Ataques con comandos ping | Denegación de servicio distribuido | 1 | 1 |
| Session Hijacking o Robos de sesión | 1 | 1 |

* **Activos Humanos**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Activos** | **Impacto** | **Amenazas** | **Vulnerabilidades** | **Probabilidad de Ocurrencia** | **Riesgo bruto** |
| Jefe Inmediato | 1 | Problemas de Salud | Datos expuestos a terceros | 2 | 2 |
| Falta de supervisión | 2 | 2 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Activos** | **Impacto** | **Amenazas** | **Vulnerabilidades** | **Probabilidad de Ocurrencia** | **Riesgo bruto** |
| Empleados | 2 | Despidos | Actualización de datos, tardías | 1 | 2 |
| Datos expuestos a terceros | 1 | 2 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Activos** | **Impacto** | **Amenazas** | **Vulnerabilidades** | **Probabilidad de Ocurrencia** | **Riesgo bruto** |
| Clientes | 2 | Cambios de información frecuentes | Saturación del sistema | 2 | 4 |
| No aceptar la política de privacidad de la organización | Campos de datos obligatorios | 1 | 2 |