



PLAN DE SEGURIDAD INFORMÁTICA

Materia: Seguridad de los Sistemas.

Profesor: Marcelo Plá.

Alumno: Pedro Navarro.

LOS BASTOS 6/11/19

PLAN DE SEGURIDAD INFORMATICA



	Elaborado	Revisado	Aprobado
NOMBRE	-Pedro Navarro	-Almada Juan	-Diaz Gabriel
CARGO	-Analista Funcional	-Gerente de Administración	-Gerente General
FIRMA			
FECHA	29/10/2019	01/10/2019	04/11/2019

Tabla de contenido

1. Alcance del Plan de Seguridad Informática.....	4
2. Caracterización del Sistema Informático.....	5
3. Resultado del Análisis de Riesgo	6
4. Políticas de Seguridad Informática.....	7
5. Responsabilidades.....	8
6. Medidas y Procedimientos.....	10
6.1. Clasificación y control de los bienes informáticos	10
6.2. Del Personal	11
6.3. Seguridad Física y Ambiental.....	11
6.4. Seguridad de Operaciones	14
6.5. Identificación, Autenticación y Control de Acceso.....	16
6.6. Seguridad ante Programas Malignos	17
6.7. Respaldo de la información.....	19
6.8 Seguridad en Redes.....	21
6.9. Gestión de Incidentes de Seguridad.....	23
7. Anexos del PSI.	26
7.1. Listado Nominal de Usuarios.....	26
7.2. Registros.....	26
7.3. Control de cambios	29

1. Alcance del Plan de Seguridad Informática

En el presente documento se realiza la elaboración de un plan de seguridad de la información para la empresa Los Bastos dedicada a la venta de productos de ropa. La elaboración de este proyecto es para la realización de un plan de seguridad acorde a las necesidades de la empresa. Para ello se hace un análisis de riesgos inicial, para identificar los activos críticos que podrían comprometer la continuidad del negocio en caso de incidente. Con este análisis inicial, posteriormente se analizarán las amenazas que pueden afectar a la empresa sujeta al análisis y con ello se obtendrán los resultados de los activos que se encuentran en riesgo potencial. A partir de estos resultados podrán diseñarse los proyectos necesarios para acercar a niveles óptimos la seguridad de los activos de la organización.

El presente Plan de Seguridad Informática es aplicable en su totalidad en las áreas de la Empresa “Los Bastos” que se encuentran en una oficina localizada en Laprida 619, Victoria Entre Ríos. Las políticas expresadas en este plan de seguridad son de obligatorio cumplimiento para todo el personal de la Empresa Los Bastos.

Enfoque del proyecto

Para realizar este análisis de riesgos se especificarán los activos de la empresa, y a partir de ahí el alcance del proyecto será reducir el riesgo de estos activos en caso de incidente o amenaza. Por tanto, el proyecto estará enfocado en identificar los activos críticos para la organización en primer lugar, a partir de la realización de un análisis de riesgos identificando las amenazas que pueden afectar a cada activo. A partir de este punto el PSI debería tener como referencia

este análisis previo con el objetivo final de ejecutar los planes adecuados orientados a mejorar los niveles de seguridad de la información en la empresa.

2. Caracterización del Sistema Informático

Actualmente, la empresa no cuenta con un departamento de sistemas. No obstante, cuenta con un soporte informático en caso de incidentes, pero únicamente en casos de emergencia, sin tener ningún plan específico ni análisis de riesgos de la empresa específica en cuestión y como soporte de áreas especializadas para guiar en la resolución de problemas e incidentes. Por lo tanto, no se dispone de ningún SGSI implantado previamente.

La empresa no cuenta con un inventario de activos actualizados ni detallados según su función o importancia dentro de la organización de la empresa. Por tanto, tampoco están clasificados para lo que dispone cada trabajador en la empresa o área de trabajo:

Gestión de activos

- Un sistema web en donde se Realiza la venta online que está vinculada con el sistema de escritorio en donde realiza la venta de productos y la publicidad de los mismos.
- El mantenimiento de estos Software es tercerizado
- Base de datos donde se salva toda la información de los sistemas, guardada en un servidor tercerizado
- Computadoras con distintos Sistemas operativo
- Herramientas Office
- Antivirus

- Conexión a internet Wifi

- Las ventas se encuentran registradas en un Excel. Todavía hay registros físicos en papel o guardados en archivos no óptimos para ser aprovechados por los sistemas.

- El personal no está capacitado para usar el sistema

3. Resultado del Análisis de Riesgo

En esta instancia del documento el objetivo es evaluar todos los activos que se encuentran en la empresa. De esta forma se definirá claramente un punto de salida de todos los activos que estén dentro de la empresa y pudiendo analizar a qué amenazas podrían estar expuestos estos activos. Una vez que disponemos de todos los activos, haremos un listado de las amenazas reales que pueden afectar a nuestros activos. Evaluando el impacto que podría sufrir la compañía en caso de que se materialicen las amenazas. Como resultado de esta fase, se obtuvieron:

Los bienes informáticos más importantes a proteger son:

- servidores/proveedores de internet.

- las computadoras

- base de datos

- red interna de la empresa

- el sistema contable

- el sistema web (Ventas y Compras)

Las amenazas más importantes a considerar de acuerdo al impacto que pudieran tener sobre la empresa son:

- La sustracción, alteración o pérdida de datos
- Fuga de información clasificada
- La introducción de programas malignos
- El ingreso a webs no autorizadas
- El empleo inadecuado de las tecnologías y sus servicios

4. Políticas de Seguridad Informática

Es necesario que la empresa tenga sus propias políticas de seguridad informática, porque ayudarán a establecer una hoja de ruta que acompañe a los empleados en su día a día. Estas políticas permitirán saber qué es aquello que está bien visto y qué es lo que nunca se debe hacer en el entorno de la empresa, evitando así situaciones complicadas que puedan poner en apuros el futuro de la empresa.

Las propuestas para mejorar el sistema de seguridad informática son:

- Se establecerán procedimientos que especifiquen quién y cómo se asignan y suspenden los derechos y privilegios de acceso a los sistemas de información.
- En caso de violación de la seguridad informática, se comunicará al encargado de inmediato para proponer las medidas correspondientes.
- Todos los bienes informáticos serán identificados y controlados físicamente hasta nivel de componentes.

-Todos los empleados de la empresa que manipulan tecnologías informáticas y de comunicaciones responden por su protección y están en la obligación de informar cualquier incidente.

El personal tiene que estar previamente preparado en los aspectos a la seguridad informática.

5. Responsabilidades

En este documento se detallan los diferentes roles y responsabilidades para llevar a cabo un correcto funcionamiento del PSI. Definimos uno a uno los diferentes roles con sus responsabilidades, teniendo en cuenta que los empleados de la compañía son reducidos y poco especializados en seguridad, ya que sus áreas no están referidas a la seguridad informática.

-Analizar los posibles riesgos introducidos por los cambios en las funciones o en el funcionamiento de la empresa para adoptar las medidas de seguridad más adecuadas.

-Aprobar las políticas, las normas y responsabilidades en materia de seguridad.

-Determinar el límite de riesgo aceptable en materia de seguridad.

-Analizar los posibles riesgos introducidos por los cambios en las funciones o en el funcionamiento de la empresa para adoptar las medidas de seguridad más adecuadas.

-Aprobar el plan de PSI.

El área de PSI se encarga de:

- Asignar roles y funciones en materia de seguridad.
- Presentar las políticas, normas y responsabilidades en materia de seguridad.
- Validar el mapa de riesgos y las acciones de mitigación propuestas.
- Validar el plan de seguridad y presentarlo para aprobación del mismo.
- Supervisar y realizar el seguimiento.
- Comprobar que se cumpla la legislación que sea aplicable en materia de seguridad.
- Promover la concienciación y formación de usuarios y liderar la comunicación necesaria.
- Revisar las incidencias más destacadas.
- Garantizar que los servicios implementados sean utilizados para los fines que fueron creados.
- Aprobar y revisar periódicamente el cuadro de comando de la seguridad y de la evolución del SGSI.

6. Medidas y Procedimientos

6.1. Clasificación y control de los bienes informáticos

Medidas:

- Se realizarán auditorías periódicas para comprobar el control de Tecnologías Informáticas.
- Cada computadora contara con un expediente técnico donde se registrarán todos los cambios que ocurran con el equipo.
- Los bienes informáticos deberán estar identificados y controlados, hasta nivel de componentes.

Procedimientos:

Procedimientos	Responsable
Capacitar al personal encargado de la protección del medio informático en materia de Seguridad Informática	Área RRHH
Mantener actualizado los sistemas Informáticos de la empresa	Área Servicio Técnico
Realizar controles sobre los bienes informáticos que se encuentran en cada área	Área Administración
Garantizar que el área donde se encuentren los medios informáticos cuente con las medidas de protección requeridas	Área de mantenimiento

6.2. Del Personal

Medidas:

-En el proceso de selección del personal que se incorpora a la empresa, en caso que su trabajo se vincule con las tecnologías informáticas, se incluirá una valoración de su nivel de preparación.

-La Dirección de Recursos Humanos será la responsable de la valoración de la preparación de cada trabajador, la que requiera el jefe de cada área correspondiente. Debe quedar documentado el resultado de esta evaluación, así como el plan de capacitación en caso que se requiera.

Selección, preparación y responsabilidad del personal respecto a la Seguridad Informática.
--

Acceso de personas a las cuentas vinculadas a la empresa.

Acceso de usuarios a Servicios instalados.
--

6.3. Seguridad Física y Ambiental

Se refiere a los controles y medidas de seguridad, alrededor y dentro de la ubicación física de los sistemas informáticos, así como los medios de acceso al mismo.

Medidas:

CPD y centro de respaldo

Ubicación y acondicionamiento físico

Control de acceso físico

Centro de Procesamiento de Datos (CPD):

-Lugar donde se ubican los recursos necesarios para el procesamiento de la información.

- Puede ser un lugar específico de gran tamaño o incluso un edificio, que albergará gran cantidad de equipamiento informático y, en general, electrónico.
- Prácticamente todas las compañías medianas o grandes tienen algún tipo de CPD. Las más grandes llegan a tener varios interconectados con distintos centros de respaldo.

CPD Centro de respaldo:

- CPD diseñado para tomar el control de otro CPD en caso de contingencias o fallo.
- Localización distinta al CPD principal.
- Equipamiento compatible con el CPD original (no necesariamente el mismo), pueden ser idénticos y datos replicados.
- El centro de respaldo debe contar con una réplica de los mismos datos con los que se trabaja en el CPD original. Ubicación y acondicionamiento

Ubicación y acondicionamiento físico

Tener en cuenta las condiciones atmosféricas adversa al decidir la ubicación y construcción.

Factores ambientales:

- Incendios.
- Inundaciones.
- Humedad.

Terremotos.

Condiciones atmosféricas a tener en cuenta:

Aspectos a considerar	Precauciones y/o medidas
Incendios	-Ubicación en área no combustible o inflamable -Disponer de un sistema antiincendios
Temperatura y humedad	-Sistema de aire acondicionado
Inundaciones	-Ubicación estanca de agua
Terremotos	- Conocer la actividad sísmica de la zona -Construcciones antisísmicas
Rayos e interferencias Electromagnéticas	- Salas protegidas mediante jaula de Faraday

Control de acceso físico

Uso de credenciales de identificación y acceso para apertura/cierre de puertas, entrada/salida a los distintos sectores de una empresa.

A una persona se le puede identificar por:

-Algo que posee: llave, tarjeta de identificación, tarjeta inteligente.

- Algo que se sabe: PIN (Personal Identificación Number), password.
- Algo que es (señas de identidad: manos, ojos, huellas digitales, voz) o saber hacer (firma escrita).

Medidas generales para todas las áreas con tecnologías informáticas:

- Todos los tomacorrientes tendrán señalizado el tipo de voltaje que suministran para evitar accidentes o incendios.
- Contar con fuentes de respaldo de energía y estabilizadores de voltaje para cada computadora.

Medidas para el ahorro de energía en todas las estaciones de trabajo:

- Activar el Modo de bajo consumo o de espera, configurando la opción de ahorro para el monitor, disco duro y la inactividad del PC.
- Habilitar el modo de hibernación.
- Desconectar los equipos después del horario laboral.

6.4. Seguridad de Operaciones

Medidas:

- El Especialista de Seguridad Informática designado no realiza tareas vinculadas con la administración de la red, los sistemas y los diferentes servicios.
- El cambio de contraseñas corresponde al Departamento de Informática.

Procedimiento de Corrección de errores y brechas de seguridad:

- Ejecutar las herramientas de seguridad autorizadas en la empresa.
- Informar al Especialista de Seguridad Informática las acciones de emergencias ejecutadas para garantizar la seguridad del sistema.
- En caso de detectarse nuevas vulnerabilidades, proponer las acciones necesarias para su evaluación y determinación de las modificaciones requeridas para su eliminación.
- Documentar en el Registro de Incidencias de Seguridad Informática las acciones ejecutadas.

Procedimiento de realización de inspecciones de Seguridad Informática:

- Confeccionar el Plan de Inspecciones de Seguridad Informática de la Entidad.
- Presentar el plan de inspecciones al gerente para su aprobación.
- Ejecutar el plan de inspecciones según la fecha planificada.
- Chequeará las tareas funcionales que debe efectuar cada cual de acuerdo a su responsabilidad.
- Realizará inspecciones independientes a cada una de las máquinas, efectuando pruebas en las que trate de violentar las medidas de seguridad.
- Se anotará los resultados en el Registro de Inspecciones.
- Confeccionar un informe con los resultados de la inspección y enviárselo al gerente de la empresa.

Responsable: Especialista de Seguridad Informática

6.5. Identificación, Autenticación y Control de Acceso

Medidas:

- Se establecerán identificadores de usuarios en las PCs, sistemas y servicios informáticos en la red.
- Los identificadores de usuarios se darán por el Administrador de la red al causar alta un usuario al trabajo con las tecnologías de la información, lo cual será notificado por el jefe de área correspondiente
- Estos identificadores serán eliminados por el Administrador de la red tan pronto el trabajador cause baja (empleando el mismo procedimiento de notificación).

Procedimiento Control de la Identificación de usuario

- Una vez que los usuarios estén creados dar acceso de personas a las Tecnologías de Información, se revisara que los identificadores que se están utilizando correspondan con la situación de los trabajadores autorizados a trabajar con las tecnologías informáticas.

Responsable: área de administración

Procedimiento autenticación de usuario:

- Las Pc contarán con contraseñas que bloqueen el acceso al Setup.
- La cuenta de administrador estará deshabilitada.
- El trabajador accederá al ordenador con el usuario que le sea asignado por el dominio. (inicial del nombre + 1er apellido)

Responsable: Área de administración

-Realizar periódicamente un Control de la Autenticación de usuarios.

Responsable: Área de administración

Responsable: Jefe de la Administración Interna

Procedimiento de autenticación de usuario en ordenadores desconectados de la red:

-Las Pc contarán con contraseñas de Inicio del SO, Setup, cuentas de administrador y usuario estándar.

-Cada usuario poseerá una contraseña para acceder a la PC en una sesión independiente.

-Habilitar el uso de protectores de pantalla con contraseña, lo que evitará que la información sea vista en momentos de inactividad y la entrada de intrusos.

Responsable: área de servicio técnico

-Los usuarios se autenticarán para hacer uso de su cuenta de usuario en la red local y los servicios autorizados.

Responsable: Usuarios

6.6. Seguridad ante Programas Malignos

Medidas:

Cada empleado de la empresa es responsable de efectuar el chequeo de todos los soportes de propiedad personal o de otra empresa que se autoricen introducir en el ordenador antes de su utilización.

- El Especialista de Seguridad Informática será el encargado de efectuar la descontaminación de las pc's de la empresa ante la aparición de programas malignos.
- La actualización del Software Antivirus de las máquinas y Servidores de la Red se realizará diariamente, de forma programada.
- La actualización del Software Antivirus en los ordenadores donde se procesa Información Oficial Clasificada es responsabilidad del Especialista de Seguridad Informática.
- Cada trabajador es responsable de comprobar la correcta actualización del Software Antivirus instalado en el ordenador a su cargo.

Procedimiento de actualización del Software Antivirus en el Servidor:

- Diariamente se descarga a las 6:00 am de forma automática desde la url: <http://antivirus/avastactualizacion/avast> la actualización del Antivirus.
 - Chequear si la actualización se descargó con efectividad.
- Responsable: usuarios.

Procedimiento de actualización del Software Antivirus en las pc's de la empresa con red local:

- Las PC Conectadas a la Red local se actualizarán diariamente a las 4:30 pm de forma programada conectándose al Servidor local.

-En caso de estar apagados los ordenadores en el horario previsto, el antivirus se actualizará apenas se encienda el equipo.

Procedimiento de descontaminación de programas malignos

-Al detectarse un programa maligno, se debe detener la actividad que se esté efectuando e informar al especialista de seguridad informática.

Responsable: Usuario del equipo infectado.

-Desconectar el cable de red de la PC e identificar qué tipo de virus es el que se aloja en la misma.

-Verificar que el Software Antivirus instalado esté debidamente actualizado. En caso de no cumplirse, actualizar el Software Antivirus y proceder con la descontaminación del equipo. De ser exitosa la descontaminación del virus poner en marcha el equipo.

-Revisar los soportes removibles que pudieron ser afectados por el virus.

-Investigar las causas de aparición del código maligno, identificar responsables y disponer acciones correctivas

-Dejar constancia del suceso en el Registro de Incidencias del ordenador.

6.7. Respaldo de la información

Medidas:

Se realizarán copias de seguridad de la información y del software que se determine y se comprobarán con regularidad.

- Garantizar un servidor con carpetas particulares para cada usuario, en la cual almacenara la información más importante de cada trabajador de la empresa
- Cada trabajador será responsable de la información que guarde en el Servidor.
- Los jefes de áreas son los responsables de organizar el almacenamiento de la información más importante de su respectiva área, definiendo la información a salvar y el trabajador encargado de esto.
- Cada área dispondrá de un disco externo para la salvaguarda de la información clasificada y/o limitada.

Procedimiento de respaldo de la Información

- Diariamente se efectúa el respaldo de la información.
- Planificación programada.
- La información importante es alojada de manera temporal en el Servidor correspondiente y luego se almacena en un disco externo.
- Controlar periódicamente el cumplimiento de este procedimiento.
Responsable: Especialista de Seguridad Informática.

Procedimiento de respaldo de la Información Oficial Clasificada.

- Crear una carpeta con la fecha en que se realiza el backup en el disco externo.
- Controlar periódicamente el cumplimiento de este procedimiento.
Responsable: Especialista de Seguridad Informática

6.8 Seguridad en Redes

Medidas:

- El Administrador de la red regularmente deberá chequear el tráfico de la red para detectar variaciones que pueden ser síntoma de mal uso de la misma.
- El Administrador de la red es quien monitorea las conexiones activas y los puertos en la red para saber qué puertos están habilitados y chequear la seguridad de los mismos.
- El Administrador de la red es quien controla la navegación en los Servidores Proxy-Firewall.
- La navegación en los Servidores Proxy-Firewall será por nombre de usuario y contraseña.
- Los Servidores Proxy-Firewall tendrán restricciones de acceso a determinados sitios Web basándose en su contenido.
- El Especialista de Seguridad Informática será el encargado de auditar los directorios para poder determinar los ataques que se realizan sobre ellos.
- El Administrador de la red deberá actualizar el sistema periódicamente con los últimos Service Pack y parches de seguridad para resguardar el sistema de las últimas vulnerabilidades conocidas.
- El Administrador de la red deberá establecer los permisos de acceso adecuados (administrador, system y usuarios autenticados).

Procedimientos

- Revisar diariamente los registros de los eventos generados.
- Ante cualquier anomalía que se detecte, investigar las causas y determinar si se está ante algún incidente de seguridad.
- Mantener la disponibilidad y la actualización de las herramientas que garantizan la auditoria de los eventos.

Responsable: Administrador de Red.

- Controlar periódicamente el cumplimiento de este procedimiento.

Responsable: Especialista de Seguridad Informática

Procedimientos de revisión de las trazas de navegación.

- Se analiza la actividad de los usuarios (Sitios visitados, fechas y horarios de las consultas, información descargada, etc.)
- Si se detecta alguna violación se realiza un informe detallado mostrando evidencia de la violación.

Responsable: Especialista de Seguridad Informática

Procedimientos de aplicación de mecanismos que implementan las políticas de Seguridad aprobadas:

- Una vez en el dominio, el equipo acatara todas las políticas aprobadas que fueron definidos

Responsable: Administrador de Red.

- Chequear periódicamente que los ordenadores cumplan con las políticas establecidas.

Responsable: Especialista de Seguridad Informática.

6.9. Gestión de Incidentes de Seguridad.

Procedimientos de acceso y/o divulgación de información no autorizada

-Informar al jefe del área, y al Especialista de Seguridad Informática.

Responsable: Persona que lo detecte

-Cancelar la operación que está realizando la diseminación de información o la eliminará del lugar en que se encuentre una vez que sea posible eliminar la evidencia.

-Chequeará los permisos y privilegios de cada usuario y de los Sistemas.

-Trata de eliminar la posibilidad de que se repita el hecho.

Responsable: Especialista de Seguridad Informática

-Crea Comisión para investigar los hechos.

-Procede a aplicar las medidas disciplinarias que correspondan.

Responsable: Jefe de Área

-Chequear periódicamente el cumplimiento de estos procedimientos

Procedimientos de acceso pirata a la red

-Informa al jefe del área y al especialista de seguridad Informática.

Responsable: Persona que lo detecte.

-Chequear periódicamente la red en busca de vulnerabilidades.

-Si el ataque procede de la propia entidad: El administrador de la red revisa los permisos otorgados, las bitácoras en los servidores (logs) y gestiona o realiza un diagnóstico interno para precisar fallas que pudieran ser aprovechadas por el atacante.

-Si el ataque procede del exterior: El administrador de la red revisa el firewall. Detecta, de existir, vulnerabilidades en los servidores efectuando o coordinando un diagnóstico.

Responsable: Administrador de red

-Se anota el hecho en el Registro de Incidencias de la Seguridad Informática.

Responsable: Especialista de Seguridad Informática

-Se investigan y analizan las vulnerabilidades en el sistema de seguridad que propiciaron los hechos. De acuerdo con la trascendencia del ataque se involucra a los órganos competentes.

-Chequear periódicamente el cumplimiento de este procedimiento en los

Procedimientos de fallos de Hardware

Informa al jefe de Área y este al jefe del Departamento de Informática Responsable: Persona que lo detecte.

-Contacta a técnicos encargados de reparación y mantenimiento del equipamiento de la empresa

Responsable: área de servicio técnico

-Si es necesario extraer el equipo y se trata de una máquina contentiva de información clasificada y/o limitada debe retirar el disco del equipo. Si esto no es posible, la información que contiene

debe ser salvada por el personal autorizado en otro soporte y borrada físicamente del disco antes de su salida de la entidad.

Responsable: área de servicio técnico

Procedimientos de fallo de Software.

- Apaga la computadora y alerta que no se use la misma
- Informa al Jefe de Área. Responsable: Persona que lo detecte.
- Restaurar utilizando el software original.
- Informar que la computadora está lista para el uso.

Responsable: Técnico.

- Notificar este hecho en el Registro de Incidencias.

Responsable: Especialista de Seguridad Informática

Procedimiento Destrucción o modificación de la información.

- Informa al Jefe de Área

Responsable: Persona que lo detecte.

- Informa al Especialista de Seguridad Informática.

Responsable: Jefe de Área.

- Trata de determinar las causas o debilidades en la Seguridad de los sistemas que propiciaron los hechos para corregirlas.

Responsable: Especialista de Seguridad Informática

- Investiga los posibles causantes para tomar las medidas disciplinarias correspondientes.

Responsable: Jefe de Área.

-Procede a orientar al personal encargado de la salva de la información afectada, su restaura a partir de las copias que se tienen.

-Hace las anotaciones en el Registro de Incidencias.

Responsable: Especialista de Seguridad Informática

7. Anexos del PSI.

7.1. Listado Nominal de Usuarios

Nombre y Apellido	Cargo	Servicio Autorizado
Gabriel Diaz	Gerente General	Control General de Cuentas de Usuario
Juan Ferreyra	Gerente de Atención al Cliente	Acceso al Servicio de Control de mediciones, e indicadores del Área de Atención al Cliente
Omar Quintana	Gerente de Servicio Técnico	Acceso al Servicio de Control de mediciones, e indicadores del Área de Servicio Técnico
Julio Pérez	Gerente de Compra/Stock	Acceso al Sistema de precio de los proveedores.

7.2. Registros

Se mostrarán cuáles fueron los métodos de medición del riesgo, de las amenazas y como calcular su nivel de impacto.

Análisis de riesgo

El cálculo de los riesgos de seguridad de información incluye normalmente el análisis y la evaluación del riesgo. El análisis del riesgo contemplará:

- 1) Identificar los activos dentro del alcance del SGSI
- 2) Identificar las amenazas a esos activos
- 3) Identificar los impactos que las pérdidas de confidencialidad, integridad y disponibilidad puedan tener sobre los activos.

IDENTIFICACIÓN DE LOS ACTIVOS

Se identificarán los activos considerados vitales por el nivel de impacto que representa a la misma en el caso de si fallara o faltara, por tal motivo se generara un listado de los mismos, como se detalla en la siguiente Tabla.

ACTIVOS PRIMARIOS
Sistema informático
Sistema web
Redes
Bases de datos
Componentes de Protección Genérica
Infraestructura
Computadoras aisladas
Sistemas clientes

IDENTIFICACIÓN DE AMENAZAS Y EVALUACIÓN DE RIESGOS

Amenazas	Riesgo	Nivel de Riesgo
Pocos insumos	1	II
Conexión a internet optima	2	I
Falta de personal	3	II
Personal no capacitado	4	II
Servidor local	5	II
Base de datos	6	II
Información no sistematizada	7	II

Para identificar los riesgos utilizaremos la siguiente metodología llamada: **Metodología general de evaluación de riesgos.**

Esto nos permite caracterizar y evaluar la magnitud de los riesgos existentes en la empresa y además nos ayuda a la toma de decisiones

Para ello definiremos una tabla con cuatro niveles:

Nivel	Significado
I	Situación crítica se requiere atención inmediata
II	Corregir adaptando medidas de control
III	Mejora
IV	Sin intervención

7.3. Control de cambios

Fecha propuesta	12/10/2019		
Empresa	Los Bastos		
Modificación propuesta	<p>Implementar licencias legales de software:</p> <p>El uso de licencias genuinas de cualquier software contribuye de manera notable en la seguridad informática para una empresa, ya que permite obtener directamente las actualizaciones que el fabricante publique.</p>		
Aceptada	Si	Fecha aceptación	17/10/2019

Fecha propuesta	19/10/2019		
Empresa	Los Bastos		
Modificación propuesta	<p>Protección del antivirus con un antimalware:</p> <p>Antimalware, está orientado a erradicar y destruir programas maliciosos que ya se han descargado y activado.</p>		
Aceptada	Si	Fecha aceptación	25/10/2019

Fecha propuesta	27/10/2019		
Empresa	Los Bastos		
Modificación propuesta	<p>Cifrar los datos de los clientes de la empresa:</p> <p>Es necesaria para mantener los datos seguros de sus clientes, cambiando la información del ordenador a códigos ilegibles.</p> <p>De esta forma, incluso si se roban los datos, será inútil para el hacker, ya que no tendrá las claves para descifrar los datos y descifrar la información.</p>		
Aceptada	Si	Fecha aceptación	01/11/2019