PROYECTO FINAL

TERNERAS DE TAMBO

Tecnicatura en tecnologías de la información

POLÍTICAS DE SEGURIDAD

GNC

Gestión de Nacimiento y Cría

Integrantes:

Emiliano Silva

Samuel Rodríguez

Agustín Rodríguez

Sebastián Mena

Contenido

[Introducción 3](#_Toc534502233)

[Objetivos 4](#_Toc534502234)

[Alcance 4](#_Toc534502235)

[Organización, normativas, manuales y procedimientos. 5](#_Toc534502236)

[Funciones de Mandos (Directores) 5](#_Toc534502237)

[Funciones de Tecnologías de la Información(TI) 5](#_Toc534502238)

[Funciones de usuarios 6](#_Toc534502239)

[Capacitaciones 6](#_Toc534502240)

[Incidentes 6](#_Toc534502241)

[Políticas de Seguridad Física. 6](#_Toc534502242)

[Seguridad del Cableado 7](#_Toc534502243)

[Ubicación y protección de los equipos 8](#_Toc534502244)

[Políticas de mantenimientos de equipos 8](#_Toc534502245)

[Políticas de Seguridad Lógica. 8](#_Toc534502246)

[Definición de contraseña 9](#_Toc534502247)

[Correo electrónico e Internet 9](#_Toc534502248)

[Internet externa 10](#_Toc534502249)

[Backup y Software de Seguridad de la red 10](#_Toc534502250)

[Políticas de seguridad para contingencia 10](#_Toc534502251)

[Incumplimiento de las políticas 11](#_Toc534502252)

## Introducción

En la década de los 80 surge la era digital con las primeras computadoras personales e internet, con el paso del tiempo el número de usuarios paso de unos usuarios a millones, hoy en día estamos en un mundo digital, donde cualquier persona con un simple celular puede realizar desde escuchar música, ver películas hasta realizar pagos desde la comodidad de su casa.

Hoy en día la información se encuentra globalizada, se puede acceder a ella desde cualquier parte del mundo.

Se ha pasado del comercio y negocios tradicionales a los electrónicos actuales (E-commerce y el E-business), donde productos de china en cuestión de horas puede estar en manos del cliente.

La información un activo de fundamental para cualquier usuario y/u organización, por lo es indispensable mantenerla segura. Por este motivo surgen las Políticas de seguridad como herramientas para evitar que los activos se vean afectados.

El objetivo de las políticas de seguridad es establecer las reglas y mecanismos de acción con respecto a recursos y servicios de las tecnologías de la información. Brindar pautas precisas y claras, para así evitar perdida de información. Para ello se debe detallar todo lo que se va a proteger y de qué forma.

La seguridad de la información será responsabilidad de la dirección de la organización en conjunto con el área de Tecnologías de la información. El departamento de TI en conjunto con la alta gerencia elaborara la normativa de usos de las tecnologías de acuerdo con las normativas legales vigentes.

Cada departamento será responsable de hacer cumplir el reglamento de uso y de funcionamiento, y en caso de que este sea violado será responsable de aplicar las medidas disciplinarias correspondientes.

La seguridad informática se refiere a la protección de infraestructuras de las tecnologías de la información y comunicación que soportan la operación de una organización, centrándose en hardware y software, como son antivirus, firewalls, detección de intrusos, entre otros elementos, además, de los enfoques técnicos los especialistas en seguridad se manejan con las vulnerabilidades y con amenazas bajo la forma de ataques, para poder mitigar los riesgos, teniendo en cuenta políticas de seguridad para poder alizar y diseñar posibles responsabilidades y reglas para evitar amenazas o minimizar los efectos.

## Objetivos

Los objetivos de estas políticas de seguridad en la información son:

* Disponibilidad: todos los componentes del sistema deberán estar disponibles cuando así lo deseen.
* Integridad: todos los componentes de la organización deben permanecer en su estado original, solo aquellos usuarios que cuenten con los permisos podrán modificarlos.
* Privacidad: solo los usuarios autorizados podrán acceder al sistema y/o datos de la organización.
* Garantizar que las normas se cumplen.
* Brindar capacitación a todo el personal interno y/o externo que tenga que trabajar para nuestra organización.
* Contar con medidas de contingencia para situaciones de urgencia (violación de la seguridad, desastres naturales, ataques mal intencionados, etc.).

Seguridad

Según la RAE:

**Seguridad**: (Del lat. *securĭtas, -ātis)*

1. f. Cualidad de seguro.

**Seguro**, ra (Del lat. *Secūrus)*

1. adj. Libre y exento de riesgo.
2. adj. Que no falla o que ofrece confianza.
3. m. Seguridad, certeza, confianza.
4. m. Lugar o sitio libre de todo peligro.

Según la definición de la Real Academia Española Seguridad es aquello que donde no hay riesgos, es aquello que ofrece confianza, con las políticas de seguridad lo que se brinda tanto a usuarios como clientes es la certeza de confianza en nuestra organización, si bien no podemos garantizar que jamás seremos atacados o que perdemos información, pero sí que tenemos medidas para afrontarlas.

## Alcance

En este documento se describirán medidas para mantener la disponibilidad, integridad y privacidad de toda la organización, para ello se definirán las responsabilidades de la pirámide (desde los mandos a los usuarios finales).

Con el fin de tener un control toda la organización, la principal regla es que exista un marco normativo, y se documente todos los procedimientos e incidentes. El trabajar de forma ordenada y siguiendo los procedimientos nos permitirá actuar rápidamente.

## Organización, normativas, manuales y procedimientos.

Las políticas de seguridad serán creadas por dirección de la organización con conjunto con cada departamento. Cada área o departamento estará integrada por profesionales y técnicos idóneos en el área; serán estos quienes realicen las normativas, manuales y procedimientos.

Las políticas deberán ser aprobadas por la dirección de la organización, toda modificación de normativa, etc. deberá ser realizada por la dirección y un profesional idóneo en el área de la norma a modificar, así evitando que estos cambios perjudiquen las políticas de seguridad.

## Funciones de Mandos (Directores)

Los mandos o directores son quienes revisan y pueden cambiar las políticas.

Entre sus funciones están:

* Controlar el cumplimiento de políticas de seguridad
* Implementar nuevas medidas.
* Gestionar las distintas áreas.
* Impartir sanciones.

## Funciones de Tecnologías de la Información(TI)

La responsabilidad de TI es mantener las gerencias, mandos, directores de las nuevas tecnologías, asegurar que las políticas de seguridad sean las adecuadas y estén actualizadas.

Entre las funciones están:

* Crear Políticas de seguridad
* Crear políticas de respaldos y áreas de almacenaje restringidas.
* Controlar los activos de la organización (HW, SW).
* Generar informes de incidentes de seguridad.
* Evaluar los riesgos de parte del factor humano y capacitar al personal en las áreas vulnerables.
* Asegurar que las políticas de seguridad se cumplan.
* Reportar a la dirección las violaciones a los normas y políticas.
* Brindar soporte técnico a los usuarios finales.
* Informar a la dirección de las tecnologías (SW o HW obsoletos)
* Actualizaciones de SW.
* Actualizaciones de antivirus.
* Políticas de seguridad en uso de HW, SO, contraseñas, e-mail.
* Brindar acceso lógico a la información.
* Generar respaldos de la información.

## Funciones de usuarios

Los usuarios es el último escalón de la pirámide de la organización, son ellos quienes usan los sistemas de la organización, dependen del área de TI para poder procesar la información.

Entre las funciones están:

* Reportar incidentes en HW y SO de sus estaciones de trabajo.
* Cumplir con las políticas de seguridad.
* Uso responsable de HW y SO.
* Uso del HW y SO con fines laborales.
* Cada usuario deberá ser responsable del uso de su credencial en la organización.
* Dispositivos que inserta en los equipos

Los equipos informáticos no podrán salir de las instalaciones sin la previa autorización.

## Capacitaciones

Las tecnologías de la información están en constante cambios, lo que ayer era tecnología nueva mañana será obsoleta, por este motivo es necesario que haya capacitación constante.

Todo usuario nuevo tendrá una capacitación par a par, esto dará un primer acercamiento al sistema y a las políticas de la compañía.

Mediante correo electrónico se enviarán los cambios de procedimientos, políticas y manuales.

## Incidentes

Todos los usuarios y o personal de la organización deberá reportar los incidentes al departamento de Tecnologías de la información.

Los incidentes se registrarán y se analizarán por el departamento de TI, todo incidente grabe se deberá reportar a la dirección.

Los incidentes medios o bajos de resuelven sin necesidad de informar a la dirección.

## Políticas de Seguridad Física.

La política contempla políticas para la seguridad física de los equipos o dispositivos y edilicia.

El acceso a las instalaciones y las distintas áreas deberá estar controlado. Todo acceso a las instalaciones de la organización por personas ajenas al activo de la empresa deberá estar autorizado por un encargado de área o la dirección de la organización.

Las personas que formen parte del activo tendrán acceso al predio por la zona de empleados, deberán registrar su entrada y salida (validación biométrica, tarjetas, etc.). El acceso a las zonas restringidas (Datacenters, etc.) por toda persona ajena al área deberá estar previamente autorizada por la dirección o encargado del área.

Para realizar el diseño de seguridad se debe considerar la estructura Física como Lógica.

Los objetivos de la seguridad física:

* Proteger los activos del T.I de los riesgos de desastres naturales y/o actos accidentales o mal intencionados.
* Minimizar la pérdida de información y garantizar la recuperación de la misma.
* Asegurar que las condiciones ambientales sean las más favorables para el buen funcionamiento de los equipos.

Seguridad física áreas y dispositivos:

* Cableados estructurales de acuerdo a las normas internacionales (Telecomunicaciones y energía)
* Seguridad estructural (Sensores de humo).
* Pararrayos en las estructuras.
* Instalación de red de incendios y extintores en cada sector.
* Salidas de emergencias bien identificadas
* Instalaciones eléctricas a de los datacenter con sistema de descarga a tierra independiente.
* Mantenimiento periódico de datacenter y sistemas de respaldo de sistema de emergencia.
* Refrigeración y sistema de ventilación independiente para los datacenter del resto de la estructura edilicia.
* Sistema de extinción de incendio por gas (extracción de oxígeno) para los datacenter evitando daños en equipos.
* Todos los equipos tendrán protección de UPS (regulador de tensión y energía).
* Cámara de seguridad en los accesos a cada sector de la empresa, en datacenter cámara para monitoreo de toda el área.
* Sistema de alarma, con sensores en todas las entradas y ventanas de la organización.
* Datacenter con cerraduras electrónicas para impedir el acceso.
* Rack del datacenter con cerraduras.
* Los interruptores de energía deben ser colocados en lugares fuera del alcance de personas externas para que no se ocasionen alguna interrupción de energía al edificio.

### Seguridad del Cableado

El cableado de red debe estar protegido por conductos como canaletas y ubicados en lugares que no obstruyan el paso a las personas para evitar daños al cable y que se vean interrumpidos los servicios de red.

La instalación de cableado eléctrico deberá ser independiente del cableado de red para evitar interferencias.

### Ubicación y protección de los equipos

En cada departamento los equipos deberán ser ubicados en lugares que no sean afectados por la lluvia, polvo o por robo.

Se prohibirá comer, beber o fumar cerca de las instalaciones de los equipos de procesamiento de información.

### Políticas de mantenimientos de equipos

Todos los equipos informáticos tanto de escritorio (Notebook, desktop), servidores y dispositivos móviles tendrán un SO asignado por el área de TI. El área de TI será responsable de actualizar tanto SO como SW. Personal ajeno al área no podrá manipular HW ni SW de los equipos. Solo el área de TI podrá realizar contrataciones de servicios de terceros para mantenimiento, la manipulación de equipos por personas ajenas del área de TI será factible de sanción para el usuario responsable del equipo.

Los equipos se actualizarán de forma centralizada por los servidores de Actualizaciones.

TI estará a cargo del mantenimiento preventivo de los servidores y computadoras personales además será realizado cada dos meses y deberá ser registrado.

Cualquier problema de falla del equipo deberá reportarse inmediatamente TI porque podría ocasionar pérdida de la información o interrupción de los servicios.

Mantenimiento correctivo de los equipos y de la red supervisado por el Jefe de Administración Sistemas.

El personal que realice pasantías en el departamento de Sistemas estará bajo la supervisión del jefe del departamento para realizar algún tipo de mantenimiento de equipos.

TI se responsabilizará de mantener la adecuada instalación de la infraestructura de red

Baja o reutilización de equipos:

Los equipos que serán sustituidos por otros deberán ser formateados y configurados nuevamente para el nuevo usuario después de sacar los respaldos respectivos, con el fin de que no exista información del antiguo dueño.

.

## Políticas de Seguridad Lógica.

El acceso a la información y sistema estará controlado por el área de tecnologías de la información, el permiso al sistema se asignará a solicitud de jefe de área o sección a la que pertenezca el usuario. Cada jefe de área tiene permisos para asignar permisos correspondientes al área a la que pertenece. Los permisos generales deberán estar autorizados por la dirección, o por cada encargado del sector a la que se solicita acceso.

El área de TI será el único que podrá asignar permisos sobre el sistema (crear usuarios en SO, instalar, desinstalar SW, sistemas de archivos).

Cada usuario será responsable de su estación de trabajo durante la jornada laboral, las contraseñas son personales e intransferibles.

El departamento de recursos humanos deberá informar los cambios de estado de los funcionarios, para darle de baja del sistema y los permisos de acceso.

TI limitara el acceso y conexión de los dispositivos extraíbles en los equipos (pendrive, celulares, tarjetas de memorias).

Todos los cambios de permisos deben ser registrado, para quitar los permisos a los usuarios deben estar autorizados por el encargado del área o dirección de la organización.

### [Definición de contraseña](https://definicion.de/contrasena/)

Una contraseña es una [clave](https://definicion.de/clave/) que brinda acceso a algo que, sin dicho código, resulta inaccesible. Se trata de un método de autentificación que apela a los datos secretos necesarios para superar una barrera de seguridad. La contraseña es una información secreta que se nos solicita para acceder a algún tipo de recurso, y que solo debe conocer el propietario del mismo.

Se debe evitar:

* La contraseña no debe contener el nombre de usuario de la cuenta, o cualquier otra información personal fácil de averiguar (cumpleaños, nombres de hijos, cónyuges, etc).
* No se deben almacenar las contraseñas en un lugar público y al alcance de los demás (encima de la mesa escrita en papel, etc…).
* No utilizar la opción de “Guardar contraseña” que en ocasiones se ofrece, para evitar reintroducirla en cada conexión.

Debemos cambiar las contraseñas cada dos o tres meses.

Se debe de usar contraseñas de 8 caracteres mínimo y debe incluir al menos una letra mayúscula, una letra minúscula, un número y un carácter especial (.-¡@)

### Correo electrónico e Internet

El servicio de internet estará asignado a ciertos usuarios finales, el acceso a internet se brindará por solicitud del área a la que pertenece el usuario o por el perfil que al que pertenezca el usuario.

El usuario será responsable de los sitios a los que ingresa, TI bloqueará los contenidos que puede ingresar dependiendo del área a la que pertenezca el usuario.

Definir de qué tamaño máximo podrá el usuario enviar y recibir archivos teniendo en cuenta el departamento en el que esté.

Instruir al usuario a no abrir correos electrónicos de remitentes desconocidos, mucho menos contestarlos o abrir archivos adjuntos que contenga el correo.

### Internet externa

Se proveerá un servicio de internet de libre navegación que estará por fuera de la red interna de la organización para uso de toda persona ajena a la organización.

### Backup y Software de Seguridad de la red

El departamento de TI será el único encargado de instalar cualquier software sobre los equipos y dispositivos de la organización.

Protección de Equipos:

* Protección contra Virus: El SW para la detección de virus deberá ser único para toda la organización y deberá estar aprobado por TI y la dirección de la organización.
* Escaneos a todo el sistema se realizará de forma periódica.
* Las actualizaciones de SW y SO se realizarán de forma programadas y con una frecuencia dada.
* Implementar políticas e implementar la protección para el acceso al trabajo remoto de usuarios que deban trabajar fuera de la organización, además este trabajo deberá ser autorizado y controlado. Se utilizara un cliente vpn para conectarse a la empresa.

Sistema de Backup:

* Se realizarán backup del sistema central (Servidores, unidades de almacenamientos) de forma periódica.
* La información más sensible y de vital importancia se respaldará a diario, y utilizando varios medios de respaldo.
* Los respaldos se alojarán en un lugar físico restringido, en una ubicación distinta al datacenter.

### Políticas de seguridad para contingencia

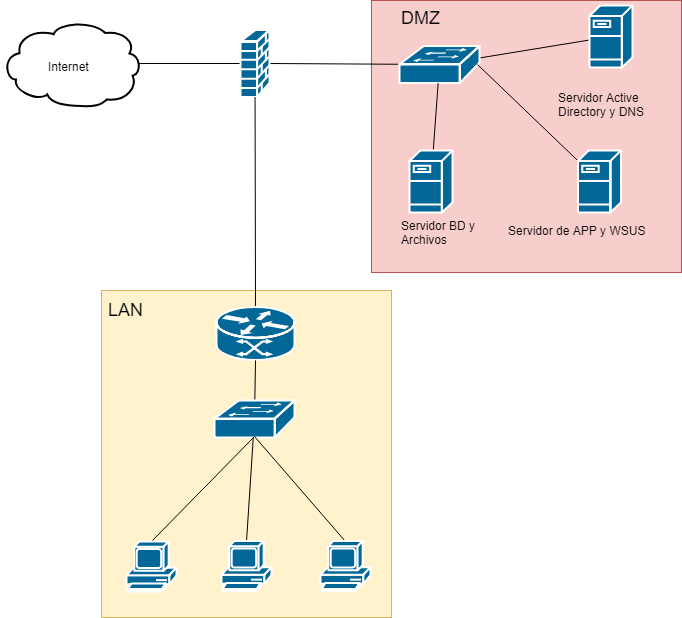
Tener planes de contingencia que nos garanticen recuperar información en el caso de que suceda algún desastre, obteniendo el menor número de pérdidas y también lograr el menor costo posible.

En el caso de que caída de las aplicaciones o de las bases de datos, se define un procedimiento para lograr la restauración y respaldo de las mismas, para tenerlas operativas lo antes posible.

Para la protección de borde de la red se utilizará un firewall de nueva generación (NGFW).

Características de los NGFW:

* Detección y prevención de intrusiones (IPS): Protección contra amenazas de red examinando flujos de tráfico (basado en firmas y en comportamientos anómalos).
* Filtrado web: Protege bloqueando acceso a páginas inapropiadas y/o peligrosas.
* Anti-SPAM: Reduce el volumen de SPAM en el perímetro.
* Anti-Virus: Protección frente amenazas a nivel de contenidos en el perímetro.
* Amenazas Persistentes Avanzadas (APT): Protección frente a APTs mediante el uso de sandboxing (local o en la nube).
* Análisis tráfico encriptado (HTTPS)
* Acceso remoto SSL/VPN



Se colocará un firewall entre el router y los switches de la capa de distribución. Su función será filtrar el trafico proveniente de la red wan e internet. Además será el encargado de realizar la conexión vpn con el resto de “sucursales”. Además cumplirá la función de DHCP

### Incumplimiento de las políticas

El incumplimiento de las políticas de seguridad deberá de ser sancionada dependiendo de la gravedad. La sanciones serán definidas por la directiva en conjunto con el departamento de TI .