**GNC**

**Gestión de Nacimiento y Cría**



**POLÍTICAS DE SEGURIDAD**

**Integrantes:**

Emiliano Silva

Samuel Rodríguez

Agustín Rodríguez

Sebastián Mena

**Índice**

[DISEÑO DE LA SEGURIDAD FISICA 3](#_Toc529023006)

[AREAS SEGURAS 3](#_Toc529023007)

[Perímetro Físico 3](#_Toc529023008)

[Controles de acceso físico 3](#_Toc529023009)

[Protección de oficinas 3](#_Toc529023010)

[SEGURIDAD DE LOS EQUIPOS 3](#_Toc529023011)

[Ubicación y protección de los equipos 3](#_Toc529023012)

[Suministros de Energía 3](#_Toc529023013)

[Seguridad del Cableado 4](#_Toc529023014)

[Mantenimiento de Equipos 4](#_Toc529023015)

[Baja o reutilización de equipos 4](#_Toc529023016)

[DISEÑO DE LA SEGURIDAD LOGICA 4](#_Toc529023017)

[Trabajo remoto 4](#_Toc529023018)

[Políticas de seguridad del hardware 4](#_Toc529023019)

[Seguridad física del equipo 4](#_Toc529023020)

[Mantenimiento de equipos 4](#_Toc529023021)

[Políticas de seguridad del software 4](#_Toc529023022)

[Políticas de seguridad para el control de acceso a los sistemas de información 4](#_Toc529023023)

[Acceso Físico 4](#_Toc529023024)

[Acceso a la información (archivos y documentos) 5](#_Toc529023025)

[Respaldos y Recuperación de archivos, aplicaciones y bases de datos 5](#_Toc529023026)

[Acceso a los servicios de red 5](#_Toc529023027)

[Administración de usuarios 5](#_Toc529023028)

[Creación de contraseñas robustas 6](#_Toc529023029)

[¿Con qué frecuencia debemos cambiar las contraseñas? 6](#_Toc529023030)

[Correo electrónico e Internet 6](#_Toc529023031)

[Políticas de seguridad para contingencia 7](#_Toc529023032)

[Concepto Seguridad Informática 7](#_Toc529023033)

[Amenazas Informáticas 7](#_Toc529023034)

[Ataques internos 7](#_Toc529023035)

[Ataques externos 7](#_Toc529023036)

[SEGURIDAD PERIMETRAL 7](#_Toc529023037)

## 

## DISEÑO DE LA SEGURIDAD FISICA

## AREAS SEGURAS

### Perímetro Físico

Los servidores deben estar en un cuarto siempre cerrado con ventilación adecuada y una buena instalación eléctrica. Solo personas autorizadas por el personal de TI podrán entrar en este cuarto.

El acceso a los diferentes departamentos deberá ser controlado en primera instancia por los guardias de seguridad y segundo por la secretaria de cada departamento en horas laborables; en horas no laborables no ingresará ninguna persona no autorizada a los departamentos.

### Controles de acceso físico

Toda persona externa que ingrese a la institución por motivos específicos deberá registrar su información en la entrada y rellenara un documento con los siguientes datos:

* Nombre
* Hora de ingreso
* Departamento al que se dirige

### Protección de oficinas

Cada departamento deberá tener un acceso principal con un lector de tarjetas magnéticas identificadoras, se contará con varios encargados en cada uno de los departamentos los cuales se encargarán de comprobar que las puertas y ventanas del departamento estén cerradas.

Se instalará un sistema de alarmas con cámaras de seguridad y reconocimiento facial, que estarán conectadas 24/7 y las alarmas se activarán automáticamente cuando el personal se haya ido y no quede nadie en el predio.

Las áreas donde se procesan datos y el departamento de TI, tienen un calendario definido para la atención al cliente, este se debe respetar o de lo contrario no se permitirá más el acceso al público.

El área donde se almacena la información sensible, deberá estar siempre bajo la protección del personal de seguridad para evitar el acceso del público y personal no deseado; y estará vigilada las 24 horas.

Cada departamento debe tener uno o varios extintores y además un sistema de detección de incendios con una alarma que avisa inmediatamente al cuerpo de bomberos, además de unos rociadores de agua en el techo que se activaran automáticamente en cuando el detector de incendios se active.

## SEGURIDAD DE LOS EQUIPOS

### Ubicación y protección de los equipos

Se deberá realizar por los menos una vez al año un monitoreo de las condiciones en las que se encuentran todos los departamentos especialmente en los de procesamiento de datos para prevenir cualquier falla en los equipos además de comprobar que estén en buen estado.

### Suministros de Energía

Se deberá contar un sistema de UPS para que en caso de un corte de electricidad se pueda seguir trabajando.

El edificio contará con pararrayos para proteger los equipos en caso de tormenta eléctrica y no exista la posibilidad de que se queme algún equipo.

### Seguridad del Cableado

El cableado de red debe estar protegido por conductos como tubos de PVC y ubicados en la parte alta del edifico para evitar daños en los cables.

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

### Mantenimiento de Equipos

Se contará con un plan de mantenimiento para evitar que el trabajo sea interrumpido por falla de algún hardware del equipo y que pueda existir pérdida de información.

Llevar un registro de daños con sus causas y posibles soluciones para estar prevenidos de futuros problemas y además poder solucionarlos de manera más rápida.

Debemos contar con un sistema de backups para asegurar la no pérdida de información sensitiva de los usuarios.

### Baja o reutilización de equipos

Los equipos que serán sustituidos por otros deberán ser formateados y configurados nuevamente para el nuevo usuario.

## 

## DISEÑO DE LA SEGURIDAD LOGICA

### Trabajo remoto

El trabajo remoto deberá ser autorizado y vigilado en caso de que los usuarios trabajen fuera de la organización.

## Políticas de seguridad del hardware

### Seguridad física del equipo

Se deberá notificar con anticipación cuando se quiera retirar un equipo de la institución para su reparación.

### Mantenimiento de equipos

TI se encargará del mantenimiento de servidores y computadoras personales, dicho mantenimiento se realizará 2 veces al año.

Cualquier problema debe reportarse inmediatamente a TI para evitar que se ocasionen perdidas de información.

Cualquier personal que realice pasantías será supervisado por el jefe de TI en el departamento al realizar cualquier tarea de mantenimiento.

### Políticas de seguridad del software

TI será el encargado de instalación y configuración de software nuevo en caso de que sea necesario para el usuario.

TI se encargará de actualizaciones y parches de seguridad del software.

### Políticas de seguridad para el control de acceso a los sistemas de información

### Acceso Físico

Los equipos deberán estar ubicados en un lugar que ofrezca buenas condiciones de seguridad.

Sólo Tecnologías de la Información y el encargado del departamento, serán quienes tengan acceso al cuarto de servidores sin ninguna restricción.

### Acceso a la información (archivos y documentos)

Las computadoras serán configuradas con contraseñas que sólo el usuario conoce y además estarán equipadas con antivirus y firewall de última generación para evitar archivos no deseados y eliminación de archivos malintencionadamente.

Instalar software de monitoreo que notifique la presencia de algún virus en el equipo, que deberá notificar inmediatamente a Tecnologías de la Información y deberá desconectar al equipo de la red hasta solucionar el problema.

Cada usuario deberá cerrar la sesión en su computador personal cuando no lo esté utilizando.

### Respaldos y Recuperación de archivos, aplicaciones y bases de datos

Tecnologías de la Información será responsable para realizar los backups de la información almacenada en las portátiles

Garantizaremos la seguridad de la información de los usuarios que se encuentra almacenada en los servidores de archivos, servidores de bases de datos, servidores de aplicaciones.

Garantizaremos la protección de la información asegurando su integridad, disponibilidad de acuerdo a sus normas establecidas.

Garantizaremos la seguridad de las bases de datos, los respaldo de las mismas y la restauración si hubiera

la necesidad.

### Acceso a los servicios de red

Se debe avisar al área de TI cuando se quieran usar los servicios de la red en horario no laboral.

El acceso a la red debe estar activo las 24 horas del día, los 365 días del año

Administración de las IP’s públicas y privadas.

Si se encuentra alguna actividad sospechosa en un computador personal, este no se podrá conectar nunca más a la red.

### Administración de usuarios

El área de TI será la encargada de la creación de los usuarios.

Cada usuario en su primer ingreso podrá cambiar su contraseña que será única e intransferible, es decir, queda prohibido que el usuario comparta su contraseña a los compañeros.

Las cuentas de los trabajadores que ya no están en la empresa serán eliminadas lo antes posible.

#### Contraseñas

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.

Es necesario invertir un poco de tiempo y esfuerzo en generar una contraseña segura. Si un usuario malintencionado consiguiera apoderarse de una contraseña podría acceder a información personal, violando la privacidad, o incluso tener acceso a servicios financieros.

La longitud de las contraseñas no debe ser inferior a ocho caracteres. A mayor longitud más difícil será de reproducir y mayor seguridad ofrecerá.

Construir las contraseñas con una mezcla de caracteres alfabéticos (donde se combinen las mayúsculas y las minúsculas), dígitos e incluso caracteres especiales (@, ¡, +, &).

Usar contraseñas diferenciadas en función del uso (por ejemplo no debe usarse la misma para una cuenta de correo que la usada para acceso a servicios bancarios).

Un buen método para crear una contraseña sólida es pensar en una frase fácil de memorizar y acortarla aplicando alguna regla sencilla.

Se deben cambiar las contraseñas regularmente. (Dependiendo de la criticidad de los datos puede ser cada X meses).

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, conyuges, ...). Tampoco una serie de letras dispuestas adyacentemente en el teclado (qwerty) o siguiendo un orden alfabético o numérico (123456, abcde, etc.)
* No se recomienda emplear la misma contraseña para todas las cuentas creadas para acceder a servicios en línea.
* Se deben evitar contraseñas que contengan palabras existentes en algún idioma (por ejemplo “campo”). Uno de los ataques más conocidos para romper contraseñas es probar cada una de las palabras que figuran en un diccionario y/o palabras de uso común.
* 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 compartir las contraseñas en Internet (por correo electrónico) ni por teléfono. En especial se debe desconfiar de cualquier mensaje de correo electrónico en el que le soliciten la contraseña o indiquen que se ha de visitar un sitio Web para comprobarla. Casi con total seguridad se tratará de un fraude. La Universidad de Almería nunca le va a solicitar ese tipo de información.
* No utilizar la opción de “Guardar contraseña” que en ocasiones se ofrece, para evitar reintroducirla en cada conexión.

### Creación de contraseñas robustas

Cuando se cree una contraseña segura, es una buena idea seguir las siguientes pautas:

No haga lo siguiente:

**No utilice solamente palabras o números** — Nunca debería utilizar únicamente letras o sólo números en una contraseña.

**No utilice palabras reconocibles** — Palabras tales como nombres propios, palabras del diccionario o hasta términos de shows de televisión o novelas deberían ser evitados, aún si estos son terminados con números.

**No utilice palabras en idiomas extranjeros**— Los programas de descifrado de contraseñas a menudo verifican contra listas de palabras que abarcan diccionarios de muchos idiomas. No es seguro confiarse en un idioma extranjero para asegurar una contraseña.

**No utilice información personal** —Si un atacante conoce quién es usted, la tarea de deducir su contraseña será aún más fácil. La lista siguiente muestra los tipos de información que debería evitar cuando esté creando una contraseña:

**No invierta palabras reconocibles** — Los buenos verificadores de contraseñas siempre invierten las palabras comunes, por tanto invertir una mala contraseña no la hace para nada más segura.

### ****¿Con qué frecuencia debemos cambiar las contraseñas?****

No cabe ninguna duda que debemos cambiar las contraseñas regularmente, buscando evitar períodos muy largos de uso de las mismas. Una buena sugerencia es**cambiar las contraseñas cada dos o tres meses.**

### Correo electrónico e Internet.

El área de TI administrara toda la información que ingrese por los correos electrónicos de los empleados y controlara la navegación de los usuarios y limitara el acceso a páginas de internet que no tienen ningún vínculo con las funciones de la empresa.

### Concepto Seguridad Informática

La seguridad informática se encarga de implementar técnicas de protección, es decir, 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.

### Amenazas Informáticas

Se define a amenaza a todo elemento o acción que sea capaz de atentar a la seguridad informática, que surgen a partir de la existencia de vulnerabilidades.

La seguridad informática se hizo presente en los años 80’s debido que se tenía la necesidad de evitar o contrarrestar los ataques informáticos, y gracias a la utilización del Internet los riesgos y amenazas fueron mayores, afectando a varias empresas y usuarios de la red, ya que la inexistencia de restricciones en el

Internet provocó que los virus, troyanos y otros códigos maliciosos se propaguen a través de correos electrónicos, publicidad o páginas web, de esta manera ayuda a que los ataques tomen el control o la información de la empresa o usuario para causar daño.

### Ataques internos

Estos ataques son iniciados por individuos o grupos de colaboradores de una empresa que conocen el negocio y tienen accesos autorizados a la red interna o incluso a cualquier Server que quiera atacar, son los más comunes y los más peligrosos

### Ataques externos

Son iniciados desde fuera de la compañía, no tienen un acceso autorizado a la red, siendo más fáciles de detectar y mitigarlos que los ataques internos, su origen es por el Internet, redes de proveedores, accesos remotos.

## SEGURIDAD PERIMETRAL

La seguridad perimetral se considera un sistema que se compone de varios elementos de tecnología, hardware y software, que actúan de manera conjunta con el fin de vigilar y proteger el perímetro, aísla a la red de amenazas, defendiendo un perímetro de seguridad. Controla todo acceso a la red interna de la empresa.

Teniendo en cuenta que la seguridad y la integridad de la información son primordiales para el funcionamiento de una empresa, nace la seguridad perimetral que es la forma para controlar el acceso y protección de los servicios informáticos.

Para la protección de la red se utilizara 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 colocara 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”

## PARCHES INFORMÁTICOS

Son programas que se encargan de modificar o hacer cambios a una aplicación para corregir errores, alterar su funcionamiento por algún motivo o agregarle funcionalidad, actualizarlas, crackearla, etc.

Los parches no pueden funcionar independientemente, por lo tanto, deben ser aplicados al programa para el cual fueron exclusivamente diseñados.

### Parches al código fuente

Parches que constan de un archivo de texto que describe modificaciones a realizar en el código fuente del programa. Estas son difundidas más que todo en el ámbito del Software Libre.

#### Parches de seguridad

Los parches de seguridad solucionan agujeros de seguridad y, no modifican la funcionalidad del programa. Los parches de seguridad son especialmente frecuentes en aplicaciones que interactúan con Internet

#### Parches de actualización

Consiste en modificar un programa con el objetivo de incorporar metodologías más nuevas. Por ejemplo, optimizar en tiempo cierto programa, añadir funcionalidades, eliminar secciones obsoletas de software, etc

## Manejo de parcheado

Dado que para estar lo menos vulnerables antes los posibles ataques, se sebe aplicar una política estricta de parcheado de todos nuestros equipos. Para ello los sistemas operativos se configurarán para que busquen los parches todos los días en las horas que menos usuarios tengamos conectados.

Para aplicar las actualizaciones a los distintos endpoint tendremos un inventario de todos nuestros equipos con los detalles de HW y SO.

A su vez dentro de los mantenimientos programados de los Datacenter se realizarán las actualizaciones a todos los dispositivos de comunicación (Switches, Router, firewall, etc.).

## Seguridad Endpoint

La seguridad endpoint enfoque para la protección de redes de computadoras que se conectan de forma remota a los dispositivos cliente. La conexión de computadoras portátiles, tabletas, teléfonos móviles y otros dispositivos inalámbricos a redes corporativas crea rutas de ataque para amenazas de seguridad. Este tipo de seguridad intenta garantizar que dichos dispositivos sigan un nivel definido de cumplimiento con los estándares de seguridad de la empresa.

## ¿Por qué una seguridad endpoint?

Existen diversos factores que contribuyen a incrementar la vulnerabilidad de los sistemas TI. Dado que los equipos portátiles de los empleados pueden contaminarse fácilmente y luego utilizarse para inyectar virus y malware directamente en el núcleo del sistema de TI de una organización; es necesaria la aplicación de nuevas estrategias que permitan proteger los entornos digitales de principio a fin.

La seguridad endpoint es un enfoque que propone soluciones de monitoreo a ordenadores conectados a la red para detectar actividades sospechosas.

## ¿En qué consiste la seguridad endpoint?

#### Identificar incluso el malware desconocido

Los cybercriminales están constantemente buscando formas de crear malwares nuevos, más complejos y difíciles de identificar. De manera que para evitar estas situaciones; una técnica de protección que se utiliza a menudo es la emulación de amenazas o el sandboxing. Los archivos sospechosos son interceptados tan pronto como llegan y son inspeccionados en un área aislada. Un archivo se bloquea tan pronto como se considera sospechoso. El Sandboxing aumenta radicalmente el potencial de detección.

#### Sandboxing inteligente

Es posible eliminar muchas formas de contaminación, por un lado, asumiendo que cada archivo adjunto, adjunto a un correo electrónico; o cada elemento descargado puede estar contaminado y, por otro, eliminando todas las amenazas potenciales antes de que lleguen al usuario. Esto se denomina extracción de amenazas: los documentos se reconstruyen utilizando únicamente elementos seguros; mientras que todo el contenido sospechoso se elimina.

#### Análisis automatizado

Incluso cuando se identifica un ataque en una fase temprana; es muy importante que comprendamos la naturaleza del ataque; cómo ocurrió y el daño que puede haber causado dentro de la empresa. Sin embargo, la complejidad del ecosistema de equipos de acceso dentro de una organización; dificulta este tipo de análisis de los incidentes de seguridad.

El análisis automatizado de incidentes, combinado con informes detallados, puede ayudar a los equipos de TI a comprender el ciclo completo de ataques y acelerar la reparación de una red contaminada.

## Directiva de uso de Internet

El acceso a Internet es un privilegio y todos los empleados deben cumplir las directivas concernientes al uso de computadora, correo electrónico e internet. Los empleados también pueden ser personalmente responsables de los daños causados por cualquier violación de esta directiva. Se requiere que todos los empleados reconozcan su recepción y confirmen que han comprendido y aceptan cumplir las reglas en adelante.

#### Uso de computadora, correo e Internet

* Se espera que los empleados utilicen Internet responsable y productivamente. El acceso a Internet está limitado a actividades relacionadas sólo con el trabajo y el uso personal no está permitido.
* Toda la información de Internet que sea redactada, transmitida y/o recibida por los sistemas informáticos se considera que pertenecen a la organización y se reconoce como parte de su información oficial. Por lo tanto, está sujeta a revelación por razones legales o para terceros apropiados.
* El correo enviado mediante el sistema de correo electrónico de la empresa no debe incluir contenido que se considere ofensivo.
* Todos los sitios y descargas pueden ser monitorizados y/o bloqueados por si se estima que son dañinos y/o no productivos para el negocio.
* La instalación de software está prohibida al menos que el área de TI lo la haya realizado.

#### El uso no aceptable de Internet incluye, pero no está limitado a:

* Enviar o publicar mensajes o imágenes discriminatorias, abusivas o amenazantes por Internet o mediante el servicio de correo de organización.
* Utilizar las computadoras para perpetrar cualquier forma de fraude, y/o pirateo de software, películas o música.
* Enviar o publicar información difamatoria para la empresa, ya sea de sus empleados o servicios que ofrece.
* Introducir software malicioso en la red de la empresa y/o poner en peligro la seguridad de los sistemas de comunicación electrónica de la organización.
* Hacer pasar las opiniones personales como representación de las de la organización.

#### El uso no aceptable de Internet:

Contenidos como Videos online, radio online, TV online, descarga de películas o algún otro programa quedan restringidos para asegurar la entrega de nuestras aplicaciones institucionales.

**Referencias:**

[**http://italred.italcol.com/intranet/politicasti/Politicas/internet.pdf**](http://italred.italcol.com/intranet/politicasti/Politicas/internet.pdf)

[**https://www.gfihispana.com/pages/sample-internet-usage-policy**](https://www.gfihispana.com/pages/sample-internet-usage-policy)

[**http://www.gb-advisors.com/es/seguridad-endpoint/**](http://www.gb-advisors.com/es/seguridad-endpoint/)

[**https://diagnosticos.wordpress.com/2010/09/05/parches-informaticos/**](https://diagnosticos.wordpress.com/2010/09/05/parches-informaticos/)

[**http://repositorio.puce.edu.ec/bitstream/handle/22000/11158/BonillaAlejandra\_SeguridadPerimetralADS.pdf?sequence=1**](http://repositorio.puce.edu.ec/bitstream/handle/22000/11158/BonillaAlejandra_SeguridadPerimetralADS.pdf?sequence=1)

[**http://bibdigital.epn.edu.ec/bitstream/15000/562/1/CD-1073.pdf**](http://bibdigital.epn.edu.ec/bitstream/15000/562/1/CD-1073.pdf)