**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 4](#_Toc529023011)

[Ubicación y protección de los equipos 4](#_Toc529023012)

[Suministros de Energía 4](#_Toc529023013)

[Seguridad del Cableado 4](#_Toc529023014)

[Mantenimiento de Equipos 4](#_Toc529023015)

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

[DISEÑO DE LA SEGURIDAD LOGICA 5](#_Toc529023017)

[Trabajo remoto 5](#_Toc529023018)

[Políticas de seguridad del hardware 5](#_Toc529023019)

[Seguridad física del equipo 5](#_Toc529023020)

[Mantenimiento de equipos 5](#_Toc529023021)

[Políticas de seguridad del software 5](#_Toc529023022)

[Políticas de seguridad para el control de acceso a los sistemas de información 5](#_Toc529023023)

[Acceso Físico 5](#_Toc529023024)

[Acceso a la información (archivos y documentos) 6](#_Toc529023025)

[Respaldos y Recuperación de archivos, aplicaciones y bases de datos 6](#_Toc529023026)

[Acceso a los servicios de red 6](#_Toc529023027)

[Administración de usuarios 6](#_Toc529023028)

[Creación de contraseñas robustas 7](#_Toc529023029)

[¿Con qué frecuencia debemos cambiar las contraseñas? 7](#_Toc529023030)

[Correo electrónico e Internet 7](#_Toc529023031)

[Políticas de seguridad para contingencia 8](#_Toc529023032)

[Concepto Seguridad Informática 8](#_Toc529023033)

[Amenazas Informáticas 8](#_Toc529023034)

[Ataques internos 8](#_Toc529023035)

[Ataques externos 8](#_Toc529023036)

[SEGURIDAD PERIMETRAL 8](#_Toc529023037)

## DISEÑO DE LA SEGURIDAD FISICA

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.

## AREAS SEGURAS

Objetivo Principal: Proteger físicamente contra el acceso no autorizado o daño a la información de los sistemas a todos los departamentos, especialmente donde se procesan datos sensibles.

### Perímetro Físico

El área de los servidores debe ser cerrada desde el piso real hasta el techo real contando con una ventilación adecuada y sus respectivas instalaciones eléctricas, donde el acceso solo será para las personas autorizadas tales como administradores de las aplicaciones, bases de datos y red.

El departamento de Tecnologías de la Información deberá crear normas a seguir para acceder y modificar al hardware. Cada empleado será responsable de sus computadores personales y no se

permitirá que personas no autorizadas a los sistemas de información tengan acceso a los computadores sin autorización. Cualquier modificación del hardware será registrada previo a la comprobación de fallo o problemas de funcionamiento con el hardware por parte del departamento de TI.

El acceso a los diferentes departamentos deberá ser controlado en primera instancia por la guardia 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

El área de información debe estar ubicada al ingreso del edificio, de tal manera que todos los usuarios que requieran información para algún trámite la obtenga en esta área y así evitar que pasen a otro departamento si no es necesario.

Toda persona externa que ingrese a la institución por motivos específicos y/o autorizados deberá registrar su información en un documento: nombre, hora de ingreso, departamento al que se dirige y además el guardia deberá retener algún documento de identidad.

La información sensible como: respaldos de datos y códigos fuentes de los sistemas de información será almacenada en un lugar de condiciones ambientales adecuadas, lejos de canalizaciones de agua y energía, se utilizarán archivadores ignífugos (resistente al calor y al fuego) y su acceso solo será permitido por las personas autorizadas en este caso al departamento de sistemas y alguna autoridad de la Institución.

### Protección de oficinas

Cada departamento deberá contar con un acceso principal con cerradura, el responsable del cuidado del edificio cerrará cada acceso principal con llave luego de que todo el personal del área se haya retirado,

además, deberá revisar las ventanas que se encuentren también cerradas.

Se debe instalar un sistema de detección de intrusos en todas las puertas y ventanas accesibles y que será activado después de cerrar los departamentos.

Las áreas donde se procesan datos y el departamento de TI, no deben ser accesibles al público todo el tiempo; deberá definirse un horario para la atención al cliente en el caso de Registro de Títulos; el ingreso de llamadas telefónicas también deberá restringirse a un determinado horario.

El área donde se almacena la información sensible, deberá estar ubicado en un lugar que no esté expuesto al acceso público.

Cada departamento debe tener un extintor de CO2 o espuma para que el personal pueda sofocar cualquier pequeño incendio si existiere.

Debido a que el hardware de cada usuario esta desprotegido por estar en los puestos de trabajo, el departamento de Tecnologías de la Información deberá organizar a los sistemas para que los usuarios finales puedan acceder a su información a través de la red local y trabajar directamente en los servidores de ficheros y servidores de aplicaciones y así mantener a los datos importantes de la Institución a salvo de errores o manipulaciones del hardware.

## SEGURIDAD DE LOS EQUIPOS

Objetivo Principal: Proteger físicamente a los equipos para reducir toda clase de daño, pérdida o acceso no autorizado a los datos y que ocasionen la interrupción a las actividades de la Institución

### 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.

De debe aplicar políticas sobre comer, beber o fumar cerca de las instalaciones de los equipos de procesamiento de información.

Se deberá realizar por los menos cuatro veces al año un monitoreo de las condiciones ambientales en los departamentos especialmente en los de procesamiento de datos para prevenir cualquier problema en los equipos.

### Suministros de Energía

El área de los servidores debe contar con un UPS para asegurar el trabajo continuo hasta que el generador de energía sea activado.

El edificio contará con una puesta a tierra para proteger de rayos a los equipos.

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

### Mantenimiento de Equipos

Se contar con un plan de mantenimiento preventivo de equipos que será calendarizado por departamentos, para evitar que el trabajo se vea interrumpido por falla de algún hardware del equipo y que exista pérdida de información.

Llevar una bitácora de daños más frecuentes en los equipos para estar prevenidos de futuros problemas con los mismos.

Debemos contar con un sistema de backups distribuidos para asegurar la información sensitiva de los usuarios finales replicando los backups entre el edificio y la casa, es decir, replicar los datos del servidor principal de archivos a otro secundario y éste deberá contar con las seguridades respectivas para los servidores.

### 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.

## DISEÑO DE LA SEGURIDAD LOGICA

Los objetivos de la Seguridad lógica son:

Definir y controlar los permisos y accesos a los programas y archivos

* Asegurar que los datos sean utilizados por el proceso adecuado y con los procedimientos correctos
* Asegurar que los datos y programas que no correspondan a un departamento sean modificados por los usuarios de dicho departamento
* Asegurar que la información trasmitida sea recibida por el destinatario al cual fue enviada.
* Asegurar que la información recibida sea la misma que fue transmitida

### Trabajo remoto

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.

## Políticas de seguridad del hardware

### Seguridad física del equipo

Todo equipo que sale de la institución debe contar con la respectiva autorización del jefe del departamento y llenar un formulario donde indique el tiempo que estará afuera de la organización, motivo y responsable del equipo, además notificar a la sección TI si el equipo es un computador para proceder a las seguridades del equipo ya establecidas.

Todo equipo que sale de la organización debe contar con la respectiva autorización del jefe del departamento y llenar un formulario donde indique el tiempo que estará afuera de la institución, motivo y responsable del equipo, además notificar al departamento de TI si el equipo es un computador para proceder a las seguridades del equipo ya establecidas.

### Mantenimiento de equipos

Tecnologías de la Información estará a cargo del mantenimiento preventivo de los servidores y computadoras personales además será realizado 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.

### Políticas de seguridad del software

Adquisición, instalación y actualización TI será quien instale software adicional a los equipos si es necesario para el usuario.

TI será el encargado de la actualización de software y de los parches de seguridad periódicamente.

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

### Acceso Físico

Los equipos deberán estar ubicados bajo condiciones que ofrezcan seguridad física, eléctricas y además que permitan el acceso físico sin ninguna restricción al personal de Tecnologías de la Información

Tecnologías de la Información será quien tenga acceso al cuarto de servidores sin ninguna restricción y en caso urgente pueden acceder las autoridades de la empresa.

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

Las portátiles serán protegidas por software de control de acceso, antivirus y firewalls para evitar que cuando salgan de la institución no regresen con problemas de mal manejo y borren programas, virus o software no deseado.

Tecnologías de la Información no será responsable de la información personal de los usuarios que se encuentre en los discos duros de cada computador.

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.

Se deberá responsabilizar al personal de contrato sobre el manejo de información a través de sus contratos.

### 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

El acceso del personal a los servicios de red y de la información en horas no laborables será con previa autorización del responsable del área y coordinado para asignar los permisos.

Otorgar permisos a los empleados para el acceso a la información y los servicios de la red dependiendo de su perfil.

Controlar que el acceso a la red y a la información esté disponible y no sea interrumpido las 24 horas del día, los 365 días del año.

Asegurar la disponibilidad de los servicios para los usuarios de acceso remoto, con previa autorización de las autoridades.

Administración de las IPs públicas y privadas.

Monitoreo de la red y si encontrara alguna actividad sospechosa ocasionado por un computador personal, lo desconectará de la red hasta solucionar el problema.

### Administración de usuarios

Tecnologías de la Información será quien cree la cuenta al nuevo usuario en la red con su respectiva identificación y autenticación.

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.

Vida útil de la clave.

Eliminar o bloquear las cuentas de las personas que ya no laboran en la institución.

Tecnologías de la Información será quien modifique las cuentas de los usuarios con previa.

#### Contraseñas

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

Tecnologías de la Información será quien administre la información que ingresa por el correo electrónico.

Controlar la navegación de los usuarios y limite el acceso a páginas de internet que no tiene

n ningún vínculo con las funciones de la empresa.

Definir qué tamaño de archivos podrá enviar y recibir cada usuario dependiendo de las normas del departamento.

El usuario no abrirá correo electrónico enviado por un remitente que no conoce, no responderá el mensaje ni mucho menos ejecutará archivos adjuntos en dichos correos.

### Políticas de seguridad para contingencia

Contar con planes de contingencia que pueda garantizar la recuperación de la información por algún desastre sin el mayor número de pérdidas y a un bajo costo.

Para el caso de un colapso total de aplicaciones o de bases de datos, se deberá definir un procedimiento de restauración de los respaldos de las mimas.

### 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

no es una tecnología, sino se considera un sistema que se compone de varios elementos de tecnología, de hardware y de software, que actúan de manera conjunta con el fin de vigilar y proteger el perímetro o “borde”, aísla a la red de entradas externas (Internet) o amenazas, defendiendo, al estilo de estrategias militares, un perímetro de seguridad se utiliza mediante el uso de equipamiento especifico configurado para realizar filtros de paquetes de datos, 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, y que los ataques y amenazas crecen constantemente ocasionando trastornos económicos,

mala imagen, funcionamiento y progreso para la empresa, nace la seguridad perimetral que es la forma para controlar el acceso y protección de los servicios informáticos.

En este proyecto para lograr la autentificación y el control de acceso se implementara un servidor radius (Remote Authentication Dial-In User Service) junto con el correspondiente servidor NPS(servidor de directivas). El servidor radius será el IAS (Internet autentication server) que viene incluido en Windows Server 2008R2. La aplicación se realizara tanto para la virtual private network(VPN) y para la red wifi.

IAS utiliza los puertos 1812 y 1645 para la autenticación y los puertos 813 y 1646 para el arqueo.

Para la protección de borde 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”

|  |  |
| --- | --- |
| Esquema de Seguridad perimetral | ? |
| Detalle de Seguridad de Endpoint y sus políticas de funcionamiento | ? |
| Detalle de funcionamiento punto III | ? |
| Flujos de tráfico LAN- WAN- DMZ | ? |
|  |  |

## PARCHES INFORMÁTICOS

**PARCHES INFORMATICOS**

Programa que se encarga de modificar o hacer cambios a una aplicación para corregir errores, alterarla 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.

Si bien los parches suelen ser desarrollados por programadores ajenos a los autores iniciales del proyecto, esto no siempre es así. Un parche puede ser aplicado tanto a un binario ejecutable como al código fuente de cualquier tipo de programa, incluso, un sistema operativo

**PARCHES BINARIO**

Estos parches consisten en una actualización del archivo ejecutable de un programa. El archivo binario es modificado para añadir los cambios o ser completamente reemplazados

### PARCHE 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.

**TIPOS DE PARCHES**

### ·         Parches de depuración

El objetivo de este tipo de parches es reparar bugs, o errores de programación que no fueron detectados a tiempo en su etapa de desarrollo.

### ·         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 cantidad de dispositivos que han venido a formar parte del ecosistema de las empresas, ha ido incrementándose. Ya sea porque para mejorar su funcionamiento, las organizaciones han decidido invertir en nueva tecnología; o porque los miembros de la empresa han comenzado a utilizar diversos equipos para simplificar su trabajo. Independientemente de la razón, este fenómeno ha incrementado los desafíos de seguridad; por lo que ha surgido la necesidad de aplicar una nueva estrategia orientada a garantizar la seguridad endpoint.

## ¿Por qué una seguridad endpoint?

Existen diversos factores que contribuyen a incrementar la vulnerabilidad de los sistemas TI. Uno de los más relevantes es la hiper-movilidad de los dispositivos tecnológicos.  Con demasiada frecuencia; los portátiles de los miembros de la organización no están protegidos por la infraestructura de seguridad de red de la empresa. Por lo tanto, son vulnerables a malware sofisticados; a dispositivos de almacenamiento externos contaminados o a contenido malicioso de sitios web.

Dado que los equipos portátiles 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. Es en este contexto en el que la seguridad endpoint se vuelve indispensable.

Cuando hablamos de endpoint nos referimos a todas las estaciones de trabajo de la empresa, incluidos los ordenadores portátiles. La seguridad endpoint por otro lado es un enfoque que propone la aplicación de soluciones que monitoreen terminales (ordenadores conectados a la red) para detectar actividades sospechosas.

Los dispositivos de usuario final son: portátiles, PC de escritorio y dispositivos móviles; y su objetivo es proporcionar visibilidad y supervisión de actividades sospechosas; como malware y ataques cibernéticos, en los dispositivos de los usuarios de las organizaciones.

## ¿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 (como macros, objetos y archivos insertados y enlaces externos) se elimina. El documento limpiado se pone a disposición del usuario después de unos segundos para que pueda utilizarlo inmediatamente y el proceso de detección no interfiera con su trabajo.

El documento original se envía a un entorno de caja de arena inteligente, configurado en una nube pública o privada, donde puede ser analizado en detalle. Si el documento está libre de contaminación, el usuario podrá descargarlo de forma segura. Este método inteligente minimiza la potencia de procesamiento y computación requerida por los equipos de acceso; a la vez que proporciona una protección óptima contra las amenazas en los archivos adjuntos de correo electrónico, las descargas o los datos copiados desde dispositivos de almacenamiento externos.

#### 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. A menudo es difícil determinar el origen de un incidente; por no hablar de la posibilidad de describir con precisión todo el ciclo seguido por el ataque y los daños causados.

Para poder analizar estos incidentes, una solución de seguridad de los equipos de acceso debe ser capaz de monitorizar continuamente los datos de ataque; lo que permitirá revelar el origen y el alcance del incidente. Los métodos actuales de control manual son excesivamente largos y laboriosos para ser implementados durante cada incidente. Por otro lado, 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. Sólo combinando la prevención avanzada de amenazas con la automatización de las tareas de recopilación y análisis de datos relacionados con los ataques; las empresas pueden proteger tanto los sistemas de los usuarios como sus núcleos de red, sin obstaculizar las operaciones.

## Directiva de uso de Internet

El uso de Internet está permitido y alentado cuando su uso apoya los objetivos del negocio. Sin embargo, el acceso a Internet es un privilegio y todos los empleados deben cumplir las directivas concernientes al uso de Computadora, Correo Electrónico e Internet. La violación de estas directivas podría suponer acciones disciplinarias y/o legales pudiendo llegar a la finalización del contrato. 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
* Las actividades relacionadas con el trabajo incluyen tareas de investigación y educativas que puedan encontrarse vía Internet que ayudarían a la función del empleado
* 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 equipamiento, servicios y tecnología utilizados para acceder a Internet son propiedad de organización y la empresa se reserva el derecho de monitorizar el tráfico de Internet y monitorizar el acceso a la información que es redactada, enviada o recibida a través de sus conexiones online
* El correo enviado mediante el sistema de correo electrónico de la empresa no debe incluir contenido que se considere ofensivo. Esto incluye, aunque no está restringido a, el uso de lenguaje/imágenes vulgares o abusivas
* 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 tales como la tecnología de mensajería instantánea está estrictamente prohibido

#### 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
* Robar, utilizar o descubrir la contraseña de un tercero sin autorización
* Descargar, copiar o piratear software y archivos electrónicos sujetos a derechos de autor o sin autorización
* Compartir material confidencial, secretos comerciales, o información propietaria fuera de la organización
* Piratear sitios web no autorizados
* Enviar o publicar información difamatoria para la empresa, sus productos/servicios, empleados y/o clientes
* 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
* Enviar o publicar cartas encadena, solicitudes, o anuncios no relacionados con los propósitos o actividades de la empresa
* Hacer pasar las opiniones personales como representación de las de la organización

#### El uso no aceptable de Internet:

El Departamento de Tecnología tiene la facultad de bloquear cualquier tráfico que dificulte el tráfico de información para la compañía.

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.

El uso de INTERNET será registrado y revisado por el Departamento de Tecnología ante cualquier requerimiento de la Contraloría Interna o Alta Gerencia de tal forma que sirva como antecedente ante una investigación.

#### Prohibiciones sobre el uso de INTERNET (Uso interno):

1. Instalar y/o usar programas para “Descargar” aplicaciones desde INTERNET hacia sus

computadores. Para evitar algún problema de contagio masivo por el uso de programas no autorizados, se prohíbe la instalación de software NO licenciado ni autorizado que ponga en riesgo la seguridad y estabilidad de la red, así como el cumplimiento de las normas legales sobre el uso de software legal.

1. El acceso a las redes de tipo social (Facebook, Instagram, Tumblr, Twitter, Snapchat, whatsapp, etc), sitios de contenido sexual, terrorismo, descargas de software libre, videos, TV Online, Radio Online o descargas de contenido en línea en general.
2. Publicar mensajes o imágenes discriminatorias, abusivas o amenazantes, así como información difamatoria de la empresa, sus productos/servicios, empleados y/o clientes.
3. Publicar comunicaciones, solicitudes, o anuncios no relacionados con los propósitos o actividades de la empresa.
4. Introducir aplicaciones de software malicioso en la red de la empresa y/o poner en riesgo la seguridad de las redes y sistemas de comunicación de la organización.
5. Se prohíbe el acceso libre y sin supervisión a las personas ajenas a la compañía a cualquiera de las redes internas de la organización. En caso que un visitante requiera hacer uso de este recurso, deberá pedir autorización de la Gerencia del área con la cual se encuentra reunido, quien le facilitará un acceso provisional a través de la red configurada para este tipo de accesos temporales.
6. El acceso a los juegos.
7. Servicios no corporativos como (Netflix, Spotify, etc).
8. Ver videos online (Youtube).

#### Políticas sobre el uso de INTERNET:

Las políticas para las restricciones de internet se realizan por el equipo de TI, para poder tener un control total del sistema. Para ello se bloquearán todos los contenidos y se irá dando acceso dependiendo de los perfiles y directivas de las gerencias. El uso de Internet para fines no institucionales estará prohibido. El contenido del tipo multimedia y redes sociales estarán prohibido. La Organización consta de 2 Redes:

1. Red Privada: es de usos interno, es donde están los equipos y usuarios de la organización y se aplica política de INTERNET no libre navegación.
2. Red Pública: Solo tiene acceso a internet, es de libre navegación, su uso está dedicado para proveedores y visitantes. Esta red no tendrá acceso a la red interna privada de la organización.