

*Factureya*<sup>®</sup> 

# Seguridad en la Información

Tel. 01 800 63 22 887

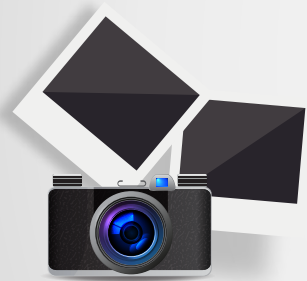
[www.factureya.com](http://www.factureya.com)

## ¿Qué es la Seguridad de la Información?

La información es un activo que como otros activos importantes tiene valor y requiere en consecuencia una protección adecuada cualquiera que sea la forma que tome o los medios por los que se comparte o almacene.



## Activos de la Información:



VISUAL



IMPRESA



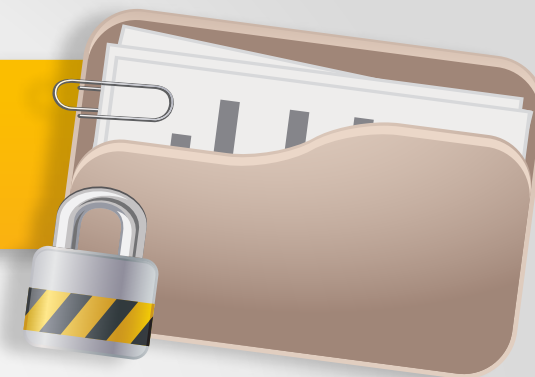
ORAL



ELECTRÓNICA



## Principios de Seguridad de la Información.



- **Confidencialidad:** La información solo debe ser accedida por el personal autorizado.
- **Disponibilidad:** La información debe encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.
- **Integridad:** Garantiza la calidad de los datos para que no puedan ser alterados.



## Prohibido



Ingresar o sustraer cualquier equipo de cómputo y dispositivos de almacenamiento.



Dejar el equipo sin bloquearlo.



Recibir y entregar mercancía, bienes y/o servicios.



Destapar equipos de cómputo.



Descargar todo tipo de Software o instalar aplicaciones



Compartir las contraseñas.



## Prohibido



Tomar fotografías videos o audios.



Ingresar o penetrar a una Red en forma ilegal o no autorizada.



Usar el correo para realizar actividades que no tengan que ver con nuestras funciones laborales.



Escribir y dejar las contraseñas en lugares de fácil acceso.



Navegar por Internet a páginas que no tengan que ver con nuestras actividades.





## Medidas de Seguridad.

- **Física:** Vela por la integridad de los equipos y por la continuidad de los suministros que necesitan.
- **Lógica:** Se encarga de la seguridad de los programas.
- **Organizacional:** Asigna funciones y responsabilidades en materia de seguridad dentro de la empresa.



## Recomendaciones para la Seguridad.

### ***Copias de Seguridad (backup).***

Es la primera y la más importante medida de seguridad.

Aunque parezca increíble, el incidente grave que se produce con más frecuencia es la pérdida de información por no haber seguido una política correcta de copias de seguridad.





## Recomendaciones para la Seguridad.



### ***Utilizar sistemas de alimentación.***

Para evitar que los procesos en curso se interrumpan bruscamente en caso de corte del suministro eléctrico y para filtrar los microcortes y picos de intensidad, que resultan imperceptibles pero que pueden provocar averías en los equipos, es muy aconsejable disponer de sistemas de alimentación ininterrumpida, al menos para servidores y equipos más importantes.



## Recomendaciones para la Seguridad.



### ***Suplantación de Identidad (Phishing).***

Es la estafa con más éxito en internet y consiste en obtener el PIN o las contraseñas mediante engaño, normalmente pidiéndolas en un correo electrónico que simula provenir de un banco o una entidad oficial.

Estos correos son siempre falsos, ya que las contraseñas no se piden nunca por este medio.



## Recomendaciones para la Seguridad.



### *Correo electrónico no deseado (Spam).*

No demos la dirección de correo a cualquiera, nos ayudará a evitar el Spam. Tampoco publiquemos direcciones personales en la WEB de la empresa, utilicemos direcciones corporativas.

Los programas de correo tienen utilidades para filtrar el **Spam**.

No enviemos propaganda por correo sin previa autorización, ya que podremos ser sancionados como Spamer por la Agencia de Protección de Datos.



## Recomendaciones para la Seguridad.



### ***Virus.***

Los **Virus** pueden llegar por correo, así que nunca abramos mensajes de origen desconocido, habrá que eliminarlos lo antes posible, ni los que contestemos, porque si lo hacemos confirmamos al que lo envió que la dirección es correcta y está activa.

Tengamos en cuenta que se suelen elegir asuntos que despiertan la curiosidad del destinatario. Otro medio de infección es la instalación de **Plugins**, contestar **NO** cuando el sistema le diga que se va a instalar un programa si no conocemos la procedencia del mismo.



## Recomendaciones para la Seguridad.



### *Plugins.*

Son pequeños programas que se descargan de internet, normalmente para poder ejecutar funciones especiales de alguna página web.



## Recomendaciones para la Seguridad.



### *Programas espía (spyware).*

Hay programas que se instalan de forma oculta en un ordenador y pueden enviar a quien los controla información contenida en el mismo e incluso las contraseñas que se tecleen en él, y también le permiten convertirlo en un Zombie y utilizarlo para sus propios fines.

Los programas anti-espías nos protegen de este software, por eso es muy importante desconfiar de aquellos que nos ofrezcan sin haberlos buscado expresamente, porque algunos programas desinstalan los espías que se encuentran en el equipo sólo para instalar uno propio.



## Recomendaciones para la Seguridad.



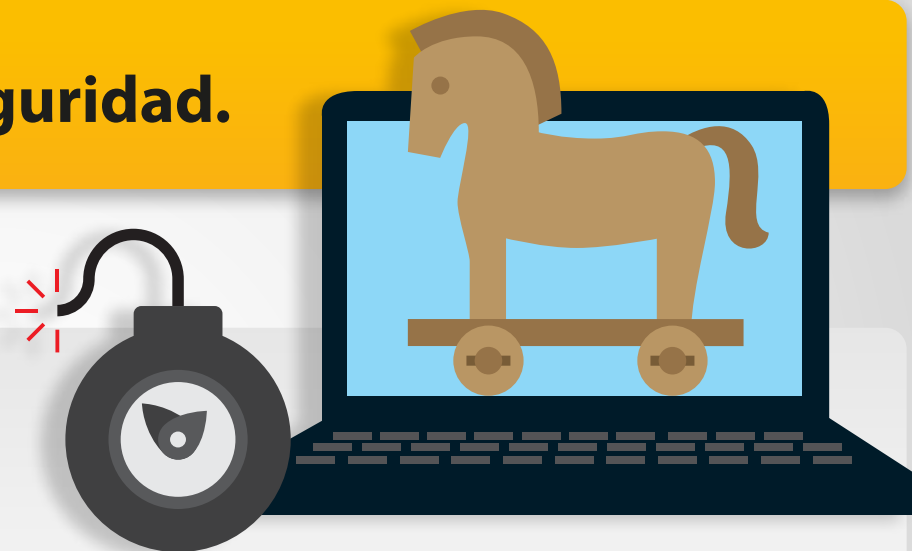
### ***Zombie.***

Es un ordenador que, sin que su propietario lo sepa, está controlado por un usuario malicioso.

Éstos suelen tener un gran número de Zombies que emplean para fines como enviar Spam, distribuir Malware o para fraudes como el Phishing.



## Recomendaciones para la Seguridad.



### ***Malware.***

Es un tipo de Software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario.



## Recomendaciones para la Seguridad.



### ***Cortafuegos (firewall).***

Son programas que analizan la información que entra y sale de un ordenador o de la red de la empresa. Evitan los ataques desde el exterior y además, permiten detectar los programas espía ya que nos avisan de que hay procesos desconocidos intentando enviar información a Internet. Junto con el antivirus es una de las medidas básicas de seguridad para los ordenadores conectados a internet.





*¿Preguntas y/o dudas?*

***¡GRACIAS!***

