Tema 4

Seguridad y confianza digital

Tema 4: Seguridad y confianza digital

Con el creciente uso de la tecnología y la interconexión de dispositivos, la información se ha convertido en un activo valioso y, por lo tanto, es necesario protegerla adecuadamente de posibles amenazas que pueden afectar a las entidades públicas.

A continuación, se brinda una introducción a lo que comprende la seguridad de la información; se describe en qué consisten las principales amenazas que la vulneran; y se exploran las mejores prácticas para proteger la información de amenazas internas y externas.

Logro de aprendizaje:

Reconocer la importancia de la seguridad de la información en las entidades públicas en el marco de la ISO 27001, con la finalidad de que el servicio civil tenga los conocimientos básicos requeridos para la protección de datos.

Contenidos:

4.1. Seguridad de la información
4.2. Amenazas a la seguridad de la información
4.3. Protección de datos

4.1. Seguridad de la información

En el proceso de transformación digital en el que vivimos, la digitalización de los procesos ha implicado que sea fundamental proteger la información y los sistemas informáticos de posibles amenazas.

La seguridad de la información se refiere a la protección de la confidencialidad, integridad y disponibilidad de los datos, conservando la privacidad de los datos personales y de las entidades públicas; todo ello sustentado en una normativa que las entidades deben cumplir, puntos que se tratarán en las siguientes líneas.

4.1.1. Seguridad de la información, ciberseguridad y seguridad digital

La seguridad se refiere a la ausencia de peligro, daño o riesgo, es decir, tener una sensación de total confianza, y esto se puede aplicar a la información.

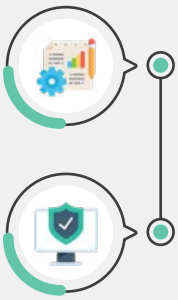
En este sentido, es importante distinguir algunos conceptos relacionados con este tema:

Tabla N° 4: Conceptos asociados a seguridad de la información	
Seguridad de la información	• Es el conjunto de medidas preventivas y reactivas que afectan al tratamiento de los datos almacenados y que permiten almacenar y proteger la información. • Incluye a las personas y a todo lo relacionado con el cumplimiento de las normas de seguridad de la información.
Ciberseguridad	• Es la práctica de defender, con tecnologías o prácticas ofensivas, las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos, de ataques maliciosos. • Comprende la perspectiva técnica de la Seguridad Digital y es un ámbito del Marco de Seguridad Digital del país.
Seguridad digital	• Es el estado de confianza en un entorno digital que resulta de la gestión y aplicación de medidas frente a riesgos que afectan su seguridad. • Se respalda en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas.

4.1.2. Normativa

La seguridad de la información de la administración pública está a cargo del Centro Nacional de Seguridad Digital (CNSD), el cual está adscrito a la Presidencia del Consejo de Ministros (PCM), a través de la Secretaría de Gobierno y Transformación Digital (SGTD).

Esta plataforma, además de ser el único punto de contacto nacional en las comunicaciones y coordinaciones con otros organismos, centros o equipos nacionales e internacionales de similar naturaleza, se encarga de:



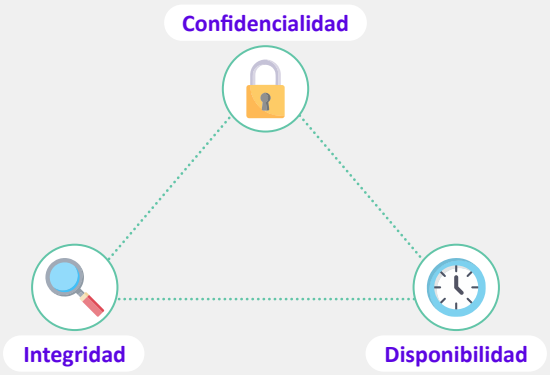
Gestionar, dirigir, articular y supervisar la operación, educación, promoción, colaboración y cooperación de la seguridad digital, con el objetivo de fortalecer la confianza digital.

Identificar, proteger, detectar, responder, recuperar y recopilar información sobre incidentes de seguridad digital para gestionarlos.

Desde el 2018, con la creación de la Ley de Gobierno Digital, se han ido implementando distintas normativas relacionadas con la seguridad de la información, la principal es la **ISO 27001 – Sistema de Gestión de Seguridad de la Información.**

Esta norma internacional otorga un marco de trabajo para los sistemas de gestión de seguridad de la información (SGSI) con el fin de proporcionar confidencialidad, integridad y disponibilidad de la información, así como el cumplimiento legal de dichos sistemas.

Gráfico N° 13: Cualidades de la información



Fuente: Elaboración propia

a. **Confidencialidad:** la información no debe ser divulgada a personas o sistemas no autorizados.

b. **Integridad:** para que la información sea válida, no debe haber sido alterada o manipulada, debe mantenerse exactamente como fue generada.

c. **Disponibilidad:** la información debe ser accesible a través de los canales adecuados y siguiendo los procesos correctos.

EJEMPLO

Un servidor civil que trabaja en una entidad pública que está certificada con la ISO 27001, está al tanto de lo que comprende y de la importancia del Sistema de Gestión de Seguridad de la Información (SGSI). Esta certificación hace protagonistas a los servidores civiles en temas de protección de datos, los beneficia a ellos y a la entidad en la que desempeñan sus funciones.

4.2. Amenazas a la seguridad de la información

Existen diversas formas en las que los sistemas informáticos pueden ser vulnerados, desde ataques de hackers hasta errores humanos en la gestión de la información. Si bien esta situación es una realidad, una manera de prevenirla es conociendo los tipos de amenazas a los que está expuesta la información y tomar medidas preventivas para protegerla, de tal manera que se garantice la seguridad de los sistemas informáticos.

4.2.1. ¿Qué es una amenaza a la seguridad de la información?

La seguridad de la información se puede ver amenazada por diferentes situaciones; sin embargo, la amenaza se debe distinguir de los conceptos de vulnerabilidad y riesgo.

a. **Amenaza:** potencial problema a la seguridad del activo (de tipo hardware, software, datos, infraestructuras de comunicaciones) que no se puede controlar directamente. La amenaza siempre existe, independientemente de cualquier contramedida.

b. **Vulnerabilidad:** debilidad o falla que puede hacer que una amenaza se vuelva realidad. Puede ser controlada.

c. **Riesgo:** probabilidad de que una amenaza se materialice y vulnere un activo de información. Afecta negativamente a la organización.

A contianuación, un ejemplo de cómo se relacionan estos conceptos:

Gráfico N° 14: Relación entre amenaza, vulnerabilidad y riesgo

Fuente: Elaboración propia

EJEMPLO

Estas situaciones también reflejan la relación de estos conceptos:

Amenaza	Vulnerabilidad	Riesgo
El atacante podría instalar un malware para robar información valiosa.	La computadora no tiene virus o está desactualizado.	Tener computadoras sin antivirus o que estén caducados.
Los atacantes podrían adivinar la contraseña del administrador de la red.	El administrador de la red usa una contraseña muy sencilla.	No capacitar a los trabajadores en el uso de contraseñas seguras.

Como se puede observar, las amenazas, las vulnerabilidades y los riesgos pueden afectar seriamente los sistemas y la información de las organizaciones, sobre todo en el entorno actual altamente digitalizado y dependiente de los servicios TI.

4.2.2. Tipos de amenazas

a. Phishing

- Tipo de ataque más recurrente a nivel mundial.
- Consiste en engañar al receptor mediante correos electrónicos que simulan ser de empresas conocidas para que revele información personal (contraseñas, número de tarjeta de crédito, etc.), con el objetivo de acceder a sus cuentas o datos bancarios.
- Recomendaciones para evitarlo:
  - No hacer clic en algún enlace sospechoso.
  - No facilitar datos personales por correo electrónico (los bancos jamás los solicitan por este medio).
  - No responder correos de personas desconocidas.
  - No hacer clic en los enlaces, sino escribir la dirección en el buscador y compararlo con el enlace real.

- Verificar que la URL tenga el candado de certificado de seguridad y la conexión HTTPS://, ya que la HTTP:// no es segura.
- Si hay dudas respecto a la validez de la información brindada por correo de una entidad financiera, consultar directamente con esta.
- Cambiar regularmente las contraseñas, sobre todo si hay sospechas de ser víctima de phishing.
- Mantener actualizado el software y usar antivirus.
- Evitar las redes wifi desconocidas.

EJEMPLO

Un servidor civil que está preparado para identificar este tipo de situaciones gracias a los comunicados del Oficial de Seguridad y Confianza Digital y las capacitaciones que recibe, desconfía si le llega un correo electrónico de su banco pidiéndole que registre nuevamente sus credenciales por la Banca por Internet mediante un enlace. Lo que hizo fue reportar esta amenaza de phishing.

b. Smishing (SMS):

- Tipo de phishing relacionado con el uso de otro canal digital como los teléfonos móviles.
- Consiste en engañar al receptor mediante mensajes de texto que simulan ser de empresas conocidas, alertándolo de que ha ganado un premio. Comúnmente, las víctimas deben responder con algún código o número especial para validar su falso premio, con ello los delincuentes capturan sus datos.
- Recomendaciones para evitarlo:
  - No hacer clic en enlaces desconocidos o sospechosos que llegan por mensaje de texto.
  - No responder a mensajes que soliciten información personal o financiera.
  - Verificar la autenticidad del remitente antes de responder un mensaje.
  - Desconfiar de mensajes que contengan errores ortográficos o gramaticales.
  - Mantener el software de seguridad y las aplicaciones actualizadas en nuestros dispositivos móviles.

c. Ingeniería social

- Técnica que consiste en ganarse la confianza del usuario para conseguir que realice algo, como ejecutar un programa malicioso, facilitar sus claves privadas, comprar en sitios web fraudulentos.
- **Técnicas:**

Pretexting: el atacante crea un escenario creíble para lograr que su víctima le brinde acceso a su computadora o espacio de trabajo con el fin de robar información o instalar un malware.

Tailgating: el atacante se aprovecha de la solidaridad o inocencia de un trabajador para evadir controles de acceso físico, como puertas electrónicas o ingresar a una organización sin autorización.

Dumpster diving (trashing): el atacante busca información relevante en la "basura digital" de un usuario.

Shoulder surfing: el atacante observa disimuladamente las contraseñas de un usuario.

Baiting: el atacante deja un dispositivo de almacenamiento físico en un lugar donde pueda ser encontrado, esperando que la víctima lo introduzca en otro para infectarlo con un código malicioso.

Vishing: el atacante llama por teléfono y trata de intimidar a alguien en su posición de poder para obtener información.

- Recomendaciones para evitarlo:
  - Verificar por otros medios la autenticidad o procedencia de un mensaje, llamada telefónica o correo.
  - No hacer excepciones ni brindar facilidades de acceso a personas no autorizadas.
  - Ser precavidos cuando se coloquen contraseñas en espacios públicos.
  - No utilizar dispositivos de almacenamiento desconocidos.

d. Malware

- Software que realiza actividades maliciosas en el equipo afectado o una red.
- **Tipos:**

Virus informático: altera el funcionamiento de un dispositivo y requiere que sea ejecutado por el usuario.

Gusano informático: su objetivo es el mismo del virus; sin embargo, no necesita ser ejecutado por el usuario, ni modificar ningún archivo para infectar la computadora.

Troyano: archivo fraudulento disfrazado para que una vez ejecutado se aproveche las vulnerabilidades del equipo.

Spyware: su objetivo es ser el espía que recolecta información del usuario o empresa sin su autorización.

Adware: no tiene la intención de dañar un equipo, sino de invadir de publicidad.

Ransomware: se secuestran datos cifrándolos, para pedir rescates económicos a cambio de liberarlos.

EJEMPLO

Un servidor civil abrió su whatsapp desde un equipo de la entidad en la que trabaja y descargó un archivo que le envió un amigo. Lamentablemente, este documento tenía virus e infectó a todos los equipos de su red.

Desde su cuenta personal, un servidor civil buscaba información sobre un viaje a Italia que desea hacer por vacaciones, y ahora no deja de ser hostigado por publicidad sobre viajes cada vez que ingresa al buscador.

e. Shadow IT

- Nombre con el que se conoce a cualquier tipo de estructura instalada en los equipos o la red, y que no está bajo la supervisión del área de TI.
- **Tipos:** Cloud, Software, Hardware y BYOD.
- Recomendaciones para evitar los ataques de malware y shadow IT:
  - Disponer de una estrategia de ciberseguridad.
  - No instalar programas de fuentes desconocidas.
  - Establecer políticas de seguridad y comunicación interna entre departamentos.
  - Establecer soluciones de seguridad informática como endpoints, firewalls, antiphishing, entre otros.

f. Suplantación de identidad

- Consiste en hacerse pasar por otra persona en internet, como la creación de un perfil falso en redes sociales o correos electrónicos.
- **Tipos:** suplantación digital, telefónica y en redes sociales, siendo este el más común en los últimos años.
- Para evitar la suplantación de identidad, se recomienda gestionar las opciones de privacidad de las redes sociales.

4.3. Protección de datos

Luego de haber revisado qué es la seguridad de la información y cuáles son las amenazas a las que está expuesta, es crucial conocer cómo proteger los datos. Para ello, las entidades públicas brindan las herramientas de ciberseguridad y capacitan a los servidores civiles en esta materia, quienes tienen el deber de ponerlas en práctica pues tienen bajo su poder un activo muy importante: la información.

4.3.1. Herramientas de ciberseguridad

Los principales problemas de seguridad de la información son los siguientes:

- Falta de autenticación de los mensajes y llamadas
- Deficientes controles de acceso
- Lectura y copia de los datos
- Alteración de los datos
- Firmas digitales falsificadas

Por tal motivo, se han diseñado herramientas que las contrarresten. Para la **autenticación de los usuarios,** control de acceso a los recursos de la red y no repudio, se utiliza PAP, CHAP, RADIUS, Certificados Digitales y Firmas Digitales.

Por su parte, **para la confidencialidad y la integridad de la información,** se utiliza la encriptación de los datos.

4.3.2. Buenas prácticas para la protección de datos

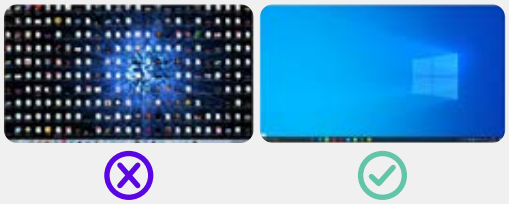
A Contraseñas

- No guardar contraseñas en lugares visibles.
- Usar contraseñas robustas: 20 caracteres a más usando combinaciones de minúsculas, mayúsculas, números y caracteres especiales (# ! @ . , : ; $ * + &).
- Cambiar las contraseñas al menos dos veces al año.
- Evitar usar una contraseña para todo.
- Emplear patrones de acceso complejos de descifrar.

B Escritorio

- Guardar en un lugar seguro los documentos y medios que contengan información pública de uso interno, pública clasificada o pública reservada.
- Bloquear los equipos de cómputo con una contraseña segura.
- Retirar de la impresora el documento utilizado, inmediatamente después de imprimir, si fuera confidencial.
- Aplicar el cierre de sesión por inactividad de los equipos de cómputo.

C Dispositivos móviles y equipos de cómputo



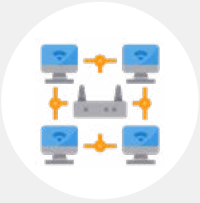
- Mantener las pantallas libres de archivos o enlaces de acceso a archivos, estos deben ubicarse en las debidas carpetas de almacenamiento.
- Bloquear la sesión de los dispositivos cuando se ausente de la estación de trabajo.
- Tener los sistemas operativos actualizados.
- Utilizar contraseñas seguras y activar el doble factor de autenticación.
- Configurar un bloqueo de pantalla.
- Configurar "copias de seguridad regular" y "borrados de datos de forma remota" (de ser posible).
- Instalar software antimalware de seguridad (antivirus).
- Evitar abrir archivos sospechosos.
- Evitar conectarse a redes inalámbricas (wifi, bluetooth) libres o de dudosa procedencia.

¿SABÍAS QUE...

...hay una protección adicional que ayuda a proteger los datos mediante su cifrado?

Se trata de colocar una contraseña a determinada información para que solo la persona que la tenga pueda descifrarlo. Esta opción está disponible en Windows PRO.

D Redes inalámbricas



- Cambiar las contraseñas del router periódicamente.
- Activar el firewall, esto impedirá que los mecanismos dañinos puedan entrar en los dispositivos. Esta protección funciona como complemento de los antivirus.
- Utilizar WPA/WPA2-PSK pues es seguro para los entornos de la red wifi de la casa, pero siempre usa una contraseña de al menos 15 caracteres.

E Teletrabajo

- Utilizar una VPN (Red privada Virtual) debido a que crea redes de comunicación entre computadoras y dispositivos con acceso restringido.
- Instalar un buen antivirus y monitorear sus actualizaciones y nuevas suscripciones.

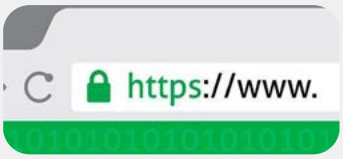
¿SABÍAS QUE...

...en el 2023 se publicó el Decreto Supremo N.° 002-2023-TR, que reglamenta la Ley N.° 31572, Nueva Ley del Teletrabajo (NLT), que fue publicada el 11 de setiembre de 2022?

El Estado formalizó con esta normativa el teletrabajo, considerando la importancia de la seguridad de la información. Ello implica que se debe capacitar continuamente a los servidores civiles sobre las amenazas que pueden perjudicar el desarrollo de los procesos y qué precauciones tomar para protegerse de ellas, además de mostrar lo perjudicial que pueden ser las amenazas informáticas para el colaborador y para la empresa.

F Navegación segura

- Activar la opción Navegación segura de las computadoras, y los dispositivos con sistema operativo Android y Apple, esto permitirá recibir alertas sobre softwares maliciosos, extensiones riesgosas, suplantación de identidad (phishing) o sitios que Google identificó como potencialmente inseguros.
- Verificar que la URL tenga el candado de certificado de seguridad y la conexión HTTPS://, ya que la HTTP:// no es segura.
- Verificar que el certificado de seguridad coincida con la URL a la que se está accediendo.
- Cuando haya enlaces acortados, poner el mouse encima para verificar la dirección de destino antes de hacerles clic.



REFLEXIONA

Los datos sensibles más comunes de un usuario son: la información sobre sus dispositivos, datos médicos, de educación, financieros, ocupación, su identidad e información en línea.

¿Tienes resguardada esta información? ¿La has publicado en tus redes sociales?

4.3.3. Autenticación

La autenticación es el proceso que usan las organizaciones para confirmar que solo las personas, servicios y aplicaciones adecuadas con los permisos correctos pueden acceder a sus recursos. Es una parte importante de la ciberseguridad porque la mayor prioridad de un infiltrado es obtener acceso no autorizado a los sistemas.

El proceso de autenticación incluye tres pasos principales:

a. **Identificación:** los usuarios establecen quiénes son a través de un nombre de usuario, normalmente.

b. **Autenticación:** es la manera en que los usuarios prueban que son quienes dicen ser. Existen diversos tipos:
   - Basada en contraseña
   - Basada en certificado
   - Biométrica
   - Multifactor: es la más eficiente pues incluye dos o más métodos de autenticación:
     - Algo que el usuario conozca (normalmente una contraseña)
     - Algo que el usuario posea (como un dispositivo de confianza que no se pueda duplicar, como el token)
     - Algo que el usuario sea (como una huella dactilar o escáner facial)

c. **Autorización:** el sistema comprueba que los usuarios tengan permisos para el sistema al que intentan acceder.

4.3.4. Gestión de ciberataques

En caso de que la amenaza cibernética se haya concretado, la administración pública cuenta con los medios necesarios para detener el ataque:

a. **Momento 1:** Las entidades despliegan todas las medidas preventivas y reactivas para afrontar el ciberataque. Una vez controlado y mitigado, el incidente debe ser reportado al Centro Nacional de Seguridad Digital (CNSD); si el incidente fue controlado, se pasará al siguiente momento.

b. **Momento 2:** Las entidades de la administración pública, los proveedores de servicios digitales del sector financiero, servicios básicos (energía eléctrica, agua y gas), salud y transporte de personas, proveedores de servicios de internet, proveedores de actividades críticas y de servicios educativos, deben:
   - Notificar al CNSD del incidente.
   - Implementar medidas de seguridad física, técnica, organizativa y legal que permitan garantizar la confidencialidad del mensaje contenido e información que se transmiten a través de sus servicios de comunicaciones.
   - Gestionar los riesgos de seguridad digital en su organización con fines de establecer controles que permitan proteger la confidencialidad, integridad y disponibilidad de la información.
   - Establecer mecanismos para verificar la identidad de las personas que acceden a un servicio digital, conforme al nivel de riesgo del mismo y de acuerdo a la normatividad vigente en materia de protección de datos personales.
   - Mantener una infraestructura segura, escalable e interoperable.

EJEMPLO

A un servidor civil le llega un correo que le ofrece duplicar sus millas por sus compras si solo actualiza sus datos mediante un enlace. Por la emoción, no dudó de esta oferta y descargó un malware, por lo que tuvo que reportar este incidente al Centro Nacional de Seguridad Digital (CNSD) para que tome las medidas reactivas pertinentes. Tras ello, la plataforma comparte lo sucedido en la Alerta integrada de seguridad digital a todas las entidades y realiza las gestiones para evitar que más equipos se contagien con el malware, además de bloquear el dominio del correo.

Cabe mencionar que si el malware hubiera sido descargado desde whatsapp web, no se hubiera podido realizar ningún bloqueo, solo alertar del hecho a los servidores civiles pues este tipo de aplicación no contiene ningún tipo de seguridad.

IMPORTANTE

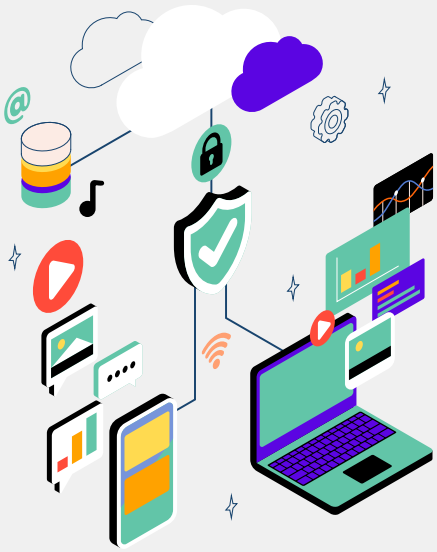
El Centro Nacional de Seguridad Digital (CNSD) es una pieza clave pues guía y asesora en temas de seguridad de información a todas las entidades públicas y otras empresas (en caso lo requieran).

Todo incidente de seguridad digital debe reportarse inmediatamente después de producido, sea que se haya concretado o no.

Resumen

ECONOMÍA DIGITAL

La seguridad de la información es el conjunto de medidas preventivas y reactivas que afectan al tratamiento de los datos almacenados y que permiten almacenar y proteger la información.



SEGURIDAD DE LA INFORMACIÓN

- La seguridad de la información de la administración pública está a cargo del Centro Nacional de Seguridad Digital (CNSD), la cual está adscrita a Presidencia del Consejo de Ministros (PCM), a través de la Secretaría de Gobierno y Transformación Digital (SGTD).
- ISO 27001 – Sistema de Gestión de Seguridad de la Información: Es la norma internacional que proporciona un marco de trabajo para los sistemas de gestión de seguridad de la información (SGSI) con el fin de proporcionar confidencialidad, integridad y disponibilidad de la información, así como el cumplimiento legal.

AMENAZAS A LA SEGURIDAD DE LA INFORMACIÓN

TIPOS DE AMENAZAS:

- **Phishing:** consiste en engañar al receptor mediante correos electrónicos que simulan ser de empresas conocidas para que revele información personal.
- **Smishing:** tipo de phishing mediante mensajes de texto.
- **Ingeniería social:** consiste en ganarse la confianza del usuario para conseguir que realice algo. Tiene diferentes técnicas (pretexting, tailgating, dumpster diving, shoulder surfing, baiting, vishing).
- **Malware:** Software que realiza actividades maliciosas en el equipo afectado o una red. Tiene diferentes tipos (virus informático, gusano informático, troyano, spyware, adware, ransomware).
- **Shadow IT:** cualquier tipo de estructura instalada en los equipos o la red, y que no está bajo la supervisión del área de TI.
- **Suplantación de identidad:** Consiste en hacerse pasar por otra persona en internet, como la creación de un perfil falso en redes sociales o correos electrónicos.

PROTECCIÓN DE DATOS

- Existen herramientas de ciberseguridad para proteger los datos:
  - Para la autenticación de los usuarios, control de acceso a los recursos de la red y no repudio: PAP, CHAP, RADIUS, Certificados Digitales y Firmas Digitales.
  - Para la confidencialidad y la integridad de la información: encriptación de los datos.
- Es fundamental cumplir con las buenas prácticas de protección de datos para el trabajo presencial así como el teletrabajo.
- La autenticación multifactor es la más eficiente pues incluye dos o más métodos de autenticación (algo que el usuario conozca, algo que el usuario posea, algo que el usuario sea).
- El Centro Nacional de Seguridad Digital es responsable de actuar en caso de ciberataques, ya sea con medidas preventivas o reactivas.
- Todos los servidores civiles tienen la responsabilidad de reportar cualquier tipo de incidente de seguridad de la información inmediatamente después de sucedido.