**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

| PROGRAMA DE FORMACIÓN | Desarrollo de habilidades digitales para experiencias seguras en línea |
| --- | --- |

| NÚMERO DEL COMPONENTE FORMATIVO | 1 |
| --- | --- |
| NOMBRE DEL COMPONENTE FORMATIVO | Ciberseguridad y Seguridad de la Información |
| BREVE DESCRIPCIÓN | El mundo digital es una realidad casi tangible en la vida actual. Cada día aumenta la cantidad de personas que están integrando el Internet a su estilo y condición de vida como productores, consumidores o espectadores, por eso el incremento en este tipo de prácticas supone una mayor exposición a riesgos de tipo informático que es necesario conocer y así evitar ser víctimas de algún tipo de fraude o delito de este tipo. |
| PALABRAS CLAVE | Amenazas, ciberseguridad, confidencialidad, información, integridad, red social, riesgo. |

| COMPETENCIA | 220501110 - Implementar el Sistema de Seguridad de la Información según modelo y estándares técnicos. | RESULTADOS DE APRENDIZAJE | 220501110 - 01 Preparar las estrategias de ciberseguridad de acuerdo a los recursos informáticos utilizados. |
| --- | --- | --- | --- |

| ÁREA OCUPACIONAL | No Aplica |
| --- | --- |
| IDIOMA | Español |

1. **TABLA DE CONTENIDO:**

**Introducción**

1. **Ciberseguridad**
   1. Marcos de referencia
   2. Triada de la Seguridad de la Información
   3. Amenazas
   4. Vulnerabilidades
   5. Activos de Información
2. **Las redes sociales**
   1. Tipos de redes sociales
   2. Usos de las redes sociales
   3. Características de seguridad en las redes sociales
3. **DESARROLLO DE CONTENIDO:**

**Introducción**

¿Qué es la ciberseguridad? ¿Qué es la seguridad de la información?

Estas preguntas y muchas más serán respondidas a lo largo del componente formativo, pero para comenzar, lo invitamos a ver el siguiente video.

Interfaz de usuario gráfica, Aplicación, PowerPoint

Descripción generada automáticamente

1. **Ciberseguridad**

**¿Qué es la ciberseguridad?**

Cano, J (2011), nos dice que es:

El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno

Y también incluye activos, bienes, servicios y datos de los dispositivos y usuarios conectados a una red; adicionalmente Cano (2011) agrega, que se pueden contar los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciber entorno en búsqueda de mantener las propiedades de seguridad en todos estos elementos de cualquier organización o persona sin importar cuál sea la red que frecuenta, su edad, su entorno y su uso.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

¿Sabía que en los últimos años el concepto de ciberseguridad se ha convertido en un estándar y en una necesidad en todas las organizaciones?

Esto se da porque cada vez más y con mayor frecuencia se recurre al uso de las tecnologías de la información y las comunicaciones para apalancar los procesos operativos junto con las propuestas de valor de los negocios.



El desarrollo y evolución de la tecnología nos lleva a hacer uso de servicios como Internet, la interconexión entre sedes y con mayor frecuencia la utilización de tecnologías de computación en la nube.



Las redes sociales y en general el Internet hacen totalmente necesario proteger toda la información que se gestiona al ingresar en cualquiera de estos recursos digitales, solo de esa forma se puede mantener monitoreadas las amenazas de las cuales se puede ser víctimas

Protegerse de los peligros de la actual coyuntura tecnológica, conlleva a diseñar y adoptar una serie de procesos que posibiliten la protección de los activos, recursos e información personal y empresarial de todos los seres digitales y para ello se recomienda la aplicación de las siguientes fases como paso inicial:

Interfaz de usuario gráfica, Aplicación, PowerPoint

Descripción generada automáticamente

Adicionalmente en el paso final de reacción se recomienda realizar en orden las siguientes actividades:

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente con confianza media

* 1. **Marcos de referencia**

Los ataques cibernéticos son cada vez más comunes y frecuentes, como se mencionó anteriormente debido a la inmersión de la tecnología en todos los procesos tanto personales como empresariales, es clara la necesidad de protección en recursos, información y activos, sin embargo el inicio se puede ser lejano y para eso se hace el siguiente planteamiento:



**¿Cómo empezar?**

Es ahí donde cobran importancia los marcos de referencia que se han venido desarrollando, porque con la adopción de estos marcos se tendrá clara y en orden, toda la información de valor y útil en el diseño de las estrategias de control y mitigación de riesgos de ciberseguridad.

Si bien se debe elegir un marco y trabajar con él, son solo una referencia y no una solución definitiva porque también es importante el enfoque del análisis de riesgos del cual se dará información más adelante. Son varios marcos, cada marco propone una serie de controles diferentes. Se debe elegir por su parte el marco indicado aplicable a su entorno y si se llegase a requerir algún ajuste se puede importar de alguno de los otros marcos y generar su propio marco de seguridad, es así como funciona esta información que con su prudente apropiación logra protección alta.

A continuación, se mencionan los marcos de referencia más utilizados y de mayor desarrollo, incluyendo algunos propósitos particulares para su adopción.

El primer marco es el dispuesto desde Norteamérica como **CSF** (*Cybersecurity Framework)*

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

El siguiente marco es el que presenta ISO denominado ISO / IEC 27001: 2013.

Creado y publicado por la Organización Internacional de Normalización (ISO), es un marco general que funciona bien para empresas de diversos tamaños en una variedad de industrias. Es similar al NIST CSF. El marco es respetado y ampliamente conocido internacionalmente. El enfoque de ISO 27001 es la protección de la confidencialidad, integridad y disponibilidad de la información en una empresa. Su filosofía se basa en la gestión de riesgos: investigar dónde están y luego tratarlos de manera sistemática tal como se presenta en la siguiente gráfica:



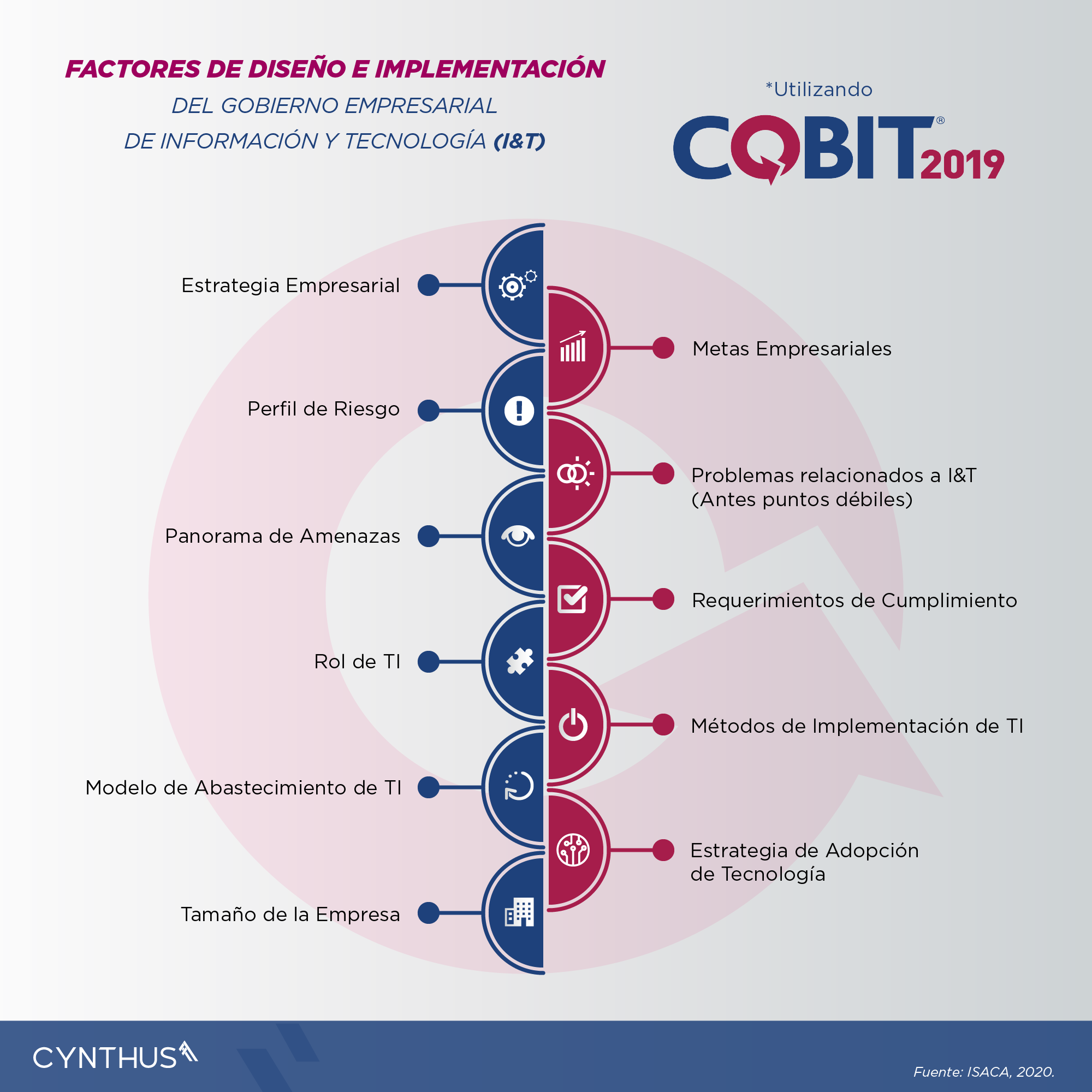
En tercer lugar se ubica la famosa COBIT que traduce Objetivos de Control para Información y Tecnologías Relacionadas. Proveniente del inglés *Control Objectives for Information and related Technology*.

COBIT fue desarrollado por ISACA, una organización global independiente sin fines de lucro que se enfoca en el gobierno de TI (Tecnologías de la Información) Este marco es similar al marco de NIST e ISO, ya que es un marco más general que la mayoría de las organizaciones pueden usar. También está enfocado en el negocio y orientado a procesos. COBIT a menudo es adoptado por auditores de empresas públicas y se utiliza como una herramienta de cumplimiento para Sarbanes-Oxley.

Es una guía de mejores prácticas, dirigida al control y supervisión de TI. Cuenta con una serie de recursos que pueden servir de modelo de referencia para la gestión de TI, incluyendo objetivos de control, mapas de auditoría, herramientas para su implementación y una guía de técnicas de gestión como se puede ver en la siguiente figura:

**Figura 1**

*Marco Cobit*



Nota. Tomado de Cynthus (2020)

El cuarto y último marco del contenido a revisar es el marco HITRUST CSF (*Health Information Trust Alliance - Cybersecurity Framework*)

HITRUST CSF fue desarrollado por *Health Information Trust Alliance* (HITRUST) y es el marco de seguridad más adoptado en la industria de la salud de los Estados Unidos. HITRUST originalmente desarrolló su CSF (*Cybersecurity Framework* – Marco de ciberseguridad) para enfocarse en elementos clave y riesgos inherentes a la industria de la salud, como las consideraciones de HIPAA (Ley de Responsabilidad y Portabilidad de Seguros de Salud) pero desde entonces han actualizado el marco con controles más amplios que se aplicarían a cualquier organización.

HITRUST CSF es un marco basado en el riesgo y el cumplimiento y se actualiza con bastante frecuencia. También se puede adaptar según una variedad de factores, que incluyen el tipo de organización, el tamaño y los sistemas, así como los requisitos reglamentarios tal como se muestra en el siguiente gráfico.

Interfaz de usuario gráfica, Aplicación, PowerPoint

Descripción generada automáticamente

* 1. **Triada de la Seguridad de la Información**

Seguridad de la información significa *proteger la información y los sistemas de información de un acceso, uso, divulgación, alteración, modificación, lectura, inspección, registro o destrucción no autorizados*

*Soriano, M. (2014)*

En el siguiente video nos presenta, de forma más completa, este concepto.

Interfaz de usuario gráfica, Aplicación, PowerPoint

Descripción generada automáticamente

* 1. **Amenazas**

Una caricatura de una persona

Descripción generada automáticamente con confianza media

Se refieren a la posibilidad que se presente algún tipo de evento se pueda, en cualquier instante de tiempo, producir un daño material o inmaterial sobre los activos informáticos y los sistemas de información. Las amenazas son consideradas como los ataques cometidos por personas internas o externas, que pueden ocasionar daños a la infraestructura tecnológica, a los sistemas de información o a la misma información que circula en la organización.

Si bien cada vez son más y más especializadas, a continuación se mencionan algunas de las amenazas más comunes y que mayor afectación provocan en nuestros recursos y medios digitales utilizados frecuentemente.

Interfaz de usuario gráfica, Aplicación, PowerPoint

Descripción generada automáticamente

* 1. **Vulnerabilidades**

Una vulnerabilidad informática es una debilidad en el software o en el hardware que permite a un posible atacante comprometer cualquiera de los elementos de la tríada de la seguridad como es la integridad, disponibilidad o confidencialidad del sistema o de los datos que procesa.

¿Por qué se presentan?

Por errores en la configuración o parametrización de las herramientas que normalmente utilizamos por ejemplo al utilizar contraseñas no seguras, al no actualizar el sistema operativo o antivirus de nuestros dispositivos.

Para clasificarlos a continuación, se mencionan algunas de las vulnerabilidades más comunes:

* + Errores en los sistemas de validación. Interfaz de usuario gráfica

    Descripción generada automáticamente con confianza media
  + Errores que permiten el acceso a directorios.
  + Errores de configuración.
  + Errores en la gestión y asignación de permisos.
  + Errores en la gestión de recursos.
  1. **Activos de información**

Este término se relaciona con todos esos elementos tecnológicos o relacionados con la tecnología que la organización utiliza para el cumplimiento de sus metas o core del negocio. Según la norma ISO/IEC 27001 se entiende como activo todo aquello que es importante y que la organización valora por lo tanto debe de protegerse.

Desde el punto de vista personal, activos informáticos serán todos aquellos elementos o herramientas tecnológicas tanto hardware (computadores, celulares, tabletas, PDA, entre otros) o elementos software como aplicaciones, correo electrónico, redes sociales, entre otras que son utilizadas dentro del contexto laboral o uso personal.

De acuerdo a la norma ISO/IEC 27001, es necesario clasificar e inventariar todos los activos de información de una empresa luego de ser identificados, esto se hace como cumplimiento al Modelo de Seguridad y Privacidad de la Información, el cual presenta la siguiente forma:

Interfaz de usuario gráfica

Descripción generada automáticamente con confianza media

La clasificación de un activo de información está dada por las propiedades de los datos, estas propiedades son:

* Confidencialidad.
* Integridad
* Disponibilidad.

Observe que siempre realizamos énfasis en la triada de la información como principios para el tratamiento de los datos; esta clasificación también revisa el impacto que tendrá cada uno de los principios en caso de ser vulnerados y el impacto de las personas o empresas en el suceso.

Icono

Descripción generada automáticamente

Debemos tener siempre presentes los riesgos informaticos, los cuales son todo tipo de vulnerabilidades, amenazas que pueden ocurrir sin previo aviso y producir numerosas pérdidas para las empresas o las personas. Los riesgos más perjudiciales son a las tecnologías de información y comunicaciones, como por ejemplo, la pérdida de datos debido a daño en los discos, virus informáticos, entre otros.

**¿Y cuáles son esos riesgos?**

Cada amenaza es diferente y no todas tienen el mismo impacto en el sistema de seguridad de los sistemas informáticos, hay exigencias elevadas y exigencias que no son tan peligrosas, pero el sistema de información y riesgo se debe encargar de todas estas amenazas de manera consciente y firme, es por eso que las partes trabajan en integrar los tipos de riesgo en tres niveles, estableciendo de esa forma la exigencia o nivel en función de la seguridad.

Interfaz de usuario gráfica, Aplicación, PowerPoint

Descripción generada automáticamente

Diagrama

Descripción generada automáticamente

**Recuerde:** analizar el riesgo es el punto inicial de trabajo en la seguridad de información puesto que ya con el riesgo identificado se decide si se elimina, se ignora, se transfiere o se logra mitigar sabiendo siempre su real impacto corporativo y personal, es decir, se hace la gestión del riesgo.

Anteriormente se estudió que existen diferentes riesgos informáticos, algunos de los más frecuentes son generados gracias al uso de dispositivos (informática) y se debe tener mucho cuidado porque algunos son de bajo riesgo pero pueden subir de nivel con rapidez y facilidad:

Interfaz de usuario gráfica, Aplicación, PowerPoint

Descripción generada automáticamente

En los protocolos de seguridad de la información ya determinamos los riesgos y las amenazas que pueden atacar tanto los recursos físicos como digitales, ahora nos preguntamos:

**¿Y cuál es el plan a seguir para el tratamiento de estos riesgos?**

Para determinar cómo tratarlo y las acciones de mitigación a realizar, tenga en cuenta lo siguiente:

Interfaz de usuario gráfica, Diagrama

Descripción generada automáticamente

* Revisar las políticas de seguridad.
* Actualizar todos los filtros y antivirus.
* Ajustar y cambiar de contraseñas de manera periódica.
* Instalar firewalls.
* Reservar datos, no compartir contraseñas.
* No compartir cuentas y contraseñas de acceso a cuentas o recursos.

Con relación a las redes sociales se dispone el siguiente paso:

* No aceptar invitaciones de personas o perfiles que no reconozca
* Revisar los contenidos antes de compartirlos para evitar problemas de seguridad

Se deben tener los controles de manera preventiva antes de tener que actuar con los correctivos.

Una vez calculado el riesgo, se debe responder con mitigación inmediata por medio de estrategias activas. A continuación se hace mención de las cuatro estrategias principales que puede usar en el caso de requerir mitigar un riesgo:



1. **Las redes sociales**



Sabía que las redes sociales son mega estructuras creadas en Internet por grupos de personas que contactan entre sí para compartir intereses en común para de esa forma crear relaciones por gustos, pasiones, intereses o necesidades. Esta es la forma más rápida de relacionarse con una persona o empresa.

Las primeras redes sociales como tal no surgieron hasta la popularización de Internet a principios del siglo XXI, en la web 2.0, cuya principal característica era dar la posibilidad a los usuarios de elaborar y publicar sus propios contenidos *online*.



Pero, gracias a la popularización y cada vez más fácil el acceso a Internet y a elementos de comunicación móviles como los teléfonos inteligentes y las tabletas, las redes sociales han tomado una gran importancia y han incrementado el uso y acceso a este tipo de plataformas, donde el usuario busca la manera de conocerse y relacionarse e incluso busca la posibilidad de ofrecer y adquirir productos, hasta utilizarlas como estrategia para la búsqueda y consecución de empleo.

**2.1 Tipos de redes sociales**

Se puede pensar equivocadamente que las redes sociales son todas iguales, pero no es así. De hecho, por lo general se dividen en diferentes tipos, de acuerdo con el objetivo de los usuarios al crear un perfil, de esa forma una misma red social puede ser útil de más de una manera.

Normalmente las redes sociales que más se usan tienen el mismo propósito, pero en realidad existen muchas otras alternativas dispuestas dependiendo del objetivo al momento del registro y crear una cuenta en ellas. La clasificación más común es:

Interfaz de usuario gráfica, Aplicación, PowerPoint

Descripción generada automáticamente

Si bien existen estas categorías de redes sociales, es importante mencionar que todas ellas fueron creadas con una visión o propósito inicial, pero que en la medida de su popularización y uso se han convertido en redes sociales que encajan perfectamente en varias de esta clasificación.

Es el caso de Facebook la cual originalmente fue creada como una red que conectara personas, en la actualidad viene siendo utilizada para ofertar productos y servicios, ofrecer entretenimiento y hasta ser un medio que facilita la publicación y contratación de oferta laboral

**2.2 Usos de las redes sociales**

Este uso está determinado por el tipo de red elegida para crear una cuenta entre muchas opciones. Los usos más comunes son:

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Al momento de crear una cuenta o registrarse en una red social, debe tener claro cuál o cuáles de las anteriores serán sus propósitos de uso. Tenga en cuenta que una misma red puede ser utilizada para uno o varios propósitos.

**2.3 Características de seguridad en las redes sociales**

Dada la proliferación o aumento de uso de las redes sociales, a continuación se mencionan algunas características de seguridad a tener en cuenta al momento de utilizarlas.

Interfaz de usuario gráfica

Descripción generada automáticamente con confianza media

1. **ACTIVIDADES DIDÁCTICAS (OPCIONALES SI SON SUGERIDAS)**

| **DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA** | |
| --- | --- |
| Nombre de la actividad | Emparejamiento entre término y definición. |
| Objetivo de la actividad | Afianzar algunos de los conceptos más importantes de la ciberseguridad y las redes sociales. |
| Tipo de actividad sugerida | Arrastrar y soltar el término con la definición que corresponde. |
| **Archivo de la actividad**  **(Anexo donde se describe la actividad propuesta)** | Anexo documento en Word llamado Actividad didáctica 1 |

1. **MATERIAL COMPLEMENTARIO**

| **Referencia APA del Material** | **Tipo de material**  **(Video, capítulo de libro,** artículo**, otro)** | **Enlace del** r**ecurso o**  a**rchivo del documento o material** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

1. **GLOSARIO**

| TÉRMINO | **SIGNIFICADO** |
| --- | --- |
| Activo | El término de activo de información se relaciona con todos esos elementos tecnológicos o relacionados con la tecnología que la organización utiliza para el cumplimiento de sus metas o core del negocio. Según la norma ISO/IEC 27001 se entiende como activo todo aquello que es importante y que la organización valora por lo tanto debe de protegerse. |
| Amenaza | Cualquier evento que puede afectar los activos de información y se relaciona, principalmente, con recursos humanos, eventos naturales o fallas técnicas. |
| ISO 27001 | Estándar de organización de estándares internacionales relacionado con la seguridad de la información. |
| Red social: | Son estructuras formadas en Internet por personas u organizaciones que se conectan a partir de intereses o valores comunes. |
| Riesgo | Es la posibilidad de que una amenaza se produzca, dando lugar a un ataque sobre un recurso o servicio tecnológico. Esto no es otra cosa que la probabilidad de que ocurra el ataque por parte de la amenaza. |
| SGSI | Sistema de gestión de Seguridad de la Información. |
| Vulnerabilidad | Es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma. |

1. **REFERENCIAS BIBLIOGRÁFICAS**

Cano, J. (2011). Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global. Sistemas (Asociación Colombiana de Ingenieros de Sistemas), 119, 4-7.

Cynthus (2020). ¿Qué hay de nuevo en COBIT® 2019? <https://www.cynthus.com.mx/que-hay-de-nuevo-en-cobit-2019/>

NIST (s.f). *Framework for Improving Critical Infrastructure Cybersecurity* https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

Soriano, M. (2014). Seguridad en redes y seguridad de la información. Obtenido de http://improvet. cvut. cz/project/download/C2ES/Seguridad\_de\_Red\_e\_Informacion. pdf.

1. **CONTROL DEL DOCUMENTO**

|  | **Nombre** | **Cargo** | **Dependencia** | **Fecha** |
| --- | --- | --- | --- | --- |
| **Autor (es)** | Henry Eduardo Bastidas Paruma | Instructor | Regional Cauca, Centro de teleinformática y producción industrial | Septiembre 2021 |
| Luis Fernando Botero Mendoza | Diseñador instruccional | Regional Distrito Capital, Centro para la industria de la comunicación gráfica | Septiembre 2021 |
| Ana Catalina Córdoba Sus | Revisora Metodológica y Pedagógica | Regional Distrito Capital – Centro para la Industria de la Comunicación Gráfica. | Septiembre 2021 |
| Rafael Neftalí Lizcano Reyes | Asesor pedagógico | Regional Santander - Centro Industrial del Diseño y la Manufactura. | Septiembre 2021 |
| Sandra Patricia Hoyos Sepúlveda | Revisión y corrección de estilo | Regional Distrito Capital – Centro para la Industria de la Comunicación Gráfica. | Septiembre 2021 |

1. **CONTROL DE CAMBIOS**

**(Diligenciar únicamente si realiza ajustes a la Unidad Temática)**

|  | **Nombre** | **Cargo** | **Dependencia** | **Fecha** | **Razón del** c**ambio** |
| --- | --- | --- | --- | --- | --- |
| **Autor (es)** |  |  |  |  |  |