
UNAD
Universidad Nacional
Abierta y a Distancia
ACREDITADA
EN ALTA CALIDAD
Ciberconciencia:
un viaje educativo
por la seguridad
digital de la UNAD
Seguridad de
la información
Universidad Nacional
Abierta y a Distancia

Universidad Nacional Abierta y a Distancia
ACREDITADA EN ALTA CALIDAD

¿Qué es la Seguridad de la Información?

Universidad Nacional Abierta y a Distancia - UNAD

Rafael Antonio Ramírez Rodríguez
Gerente de Plataformas e Infraestructura Tecnológica
gerencia.plataformas@unad.edu.co
601 - 3443700 Ext. 1696

Carlos Andrés Materon
Coordinador Infraestructura Tecnológica
carlos.materon@unad.edu.co
601 - 3443700 Ext. 1655

Leonardo Montilla Malaver
Oficial de Seguridad de la Información
seguridad.informacion@unad.edu.co
601 - 3443700 Ext. 1687

Tatiana Isabel Herazo Usta
Administración Copias de Respaldo
tatiana.herazo@unad.edu.co
601 - 3443700 ext. 1685

Ivonne Faride Acero Palomares
Calidad, Proyectos y Contratos
ivonne.acero@unad.edu.co
601 - 3443700 ext. 1649

Contenido

Introducción

La seguridad informática y la seguridad de la información son términos estrechamente relacionados que se refieren a la protección de los sistemas informáticos y los datos que contienen.

Para Romero et al (2018) no se deben confundir los conceptos de seguridad informática y la seguridad de la información ,la seguridad informática se encarga de la seguridad del medio informático, la informática para estos autores es la ciencia que se encarga de los procesos, técnicas y métodos que buscan procesar, almacenar y transmitir la información, mientras tanto la seguridad de la información no se preocupa solo por el medio informático, se preocupa por todo aquello que pueda contener información. La principal tarea de la seguridad informática es la de minimizar los riesgos, en este caso provienen de muchas partes, puede ser de la entrada de datos, del medio que transporta la información, del hardware que es usado para transmitir y recibir, los mismos usuarios y hasta por los mismos protocolos que se están implementando pero siempre la tarea principal es minimizarlos riesgos para obtener mejor y mayor seguridad, lo que debe contemplar la seguridad se puede clasificar en tres dimensiones que son:

- **Los usuarios**: Son considerados como el eslabón más débil de la cadena ya que a las personas es imposible de controlar.
- **La información**: Se considera como el centro de la seguridad informática ya que es lo que se desea proteger, es el principal activo.
- **La infraestructura**: Puede ser uno de los medios más controlados, pero eso no implica que sea el que corre menos riesgos, dependerá de los procesos que se manejen, se deben considerar problemas complejos como los de un acceso no permitido, robo de identidad hasta los daños más comunes como robo del equipo o desastres naturales.

Con esta información periódica, esperamos mantenerlos informados y actualizados a fin de aportar de esta forma a los programas de gestión del riesgo, darles a conocer nuevos avances de ciberseguridad y establecer líneas de prevención y gestión en el control y seguimiento de los riesgos de la información mediante estrategias de prevención del riesgo o su mitigación, lo anterior permitirá optimizar la seguridad informática y preservar nuestro activo primordial como es la información institucional. Se Define igualmente que la seguridad podría ser catalogada como la ausencia de riesgo, la definición de este término involucra cuatro acciones que siempre están inmersas en cualquier asunto de seguridad como son:

- Prevención del riesgo
- Transferir el riesgo
- Mitigar el riesgo
- Aceptar el riesgo

Estas acciones son algo que se debe considerar sin importar el área a cualquier intento de tener mejor o mayor seguridad en cualquier tema que se requiera.

Objetivo

La cartilla de seguridad de la información tiene como objetivo:

Brindar una información veraz y oportuna de las estrategias didácticas y tecnológicas que permitan a la comunidad universitaria conocer y utilizar las metodologías más apropiadas para prevenir los riesgos que puedan afectar la seguridad de la información como el bien más preciado de la institución en todos sus ámbitos.

Alcance

El alcance de la guía y la información que brinda está diseñada para ser aplicadas a toda la comunidad Unadista, con un enfoque particular en el marco académico. Esto incluye estudiantes, docentes y personal administrativo. La cartilla aborda una amplia gama de temas, desde la protección de datos personales hasta la seguridad en el uso de dispositivos y redes.

1. La Gestión del Riesgo

El método que está destinado a determinar, analizar, valorar y clasificar el riesgo para buscar mecanismos de control del mismo riesgo a este aspecto se le denomina gestión del riesgo.

Un concepto ampliamente relacionado con la gestión del riesgo es el concepto de ACTIVO que es un concepto abordado en los sistemas contables y en este caso se refiere a la información como un activo por su gran valor en sí misma. Otro concepto es la AMENAZA que es considerada como todo aquello que puede provocar daño al activo y la vulnerabilidad que se refiere a las inseguridades que posee el activo o información debido a problemas técnicos o a aspectos de procedimiento y el RIESGO que es la consecuencia de que una amenaza se produzca en razón de la presencia de una vulnerabilidad. Una gestión eficiente del riesgo está relacionada con la mejora continua por cuanto es consistente con la dinámica del riesgo y que se sustenta en la necesidad de hacer presencia durante todo el proceso, y se debe evaluar la gestión del riesgo a partir de métodos, funciones y responsabilidades, las herramientas y tecnologías en la organización

2. Amenazas y Riesgos en la Seguridad de la Información

Las amenazas se pueden clasificar en las siguientes clases:

- **Origen físico:** Son amenazas que provienen de desastres ambientales, degradación o fallas físicas en el sistema GIS.
- **Nivel usuario:** Estas amenazas están enfocadas hacia los errores que pueda causar un usuario sobre los activos del sistema GIS.
- **Nivel Hardware:** Estas amenazas están enfocadas a diferentes fallas que puedan presentar los componentes de hardware del sistema.
- **Nivel Datos:** Estas amenazas se enfocan en la información y datos del sistema GIS que pueden estar expuestos a un acceso no autorizado, una alteración entre otros.
- **Nivel Software:** Dentro de eta clase se encuentran amenazas enfocadas a errores de diseño, pruebas e implementación de software del sistema GIS.
- **Nivel Infraestructura:** dentro de esta clase se encuentran amenazas enfocadas a problemas de organización en la parte de infraestructura que pueden ocasionar perjuicios al sistema GIS.
- **Nivel Políticas:** Estas amenazas están enfocadas en la falta de normas y reglas de la organización de las cuales pueden llegar a tener un gran riesgo los activos del sistema.
- **Nivel Redes:** Estas amenazas están enfocadas a fallas de seguridad en el acceso y transmisión al través de la red del sistema.
- **Nivel Acceso:** Dentro de esta clase se presentan amenazas de acceso de personal no autorizado al sistema.

2.1. Ejemplos de Amenazas y Riesgos

En el contexto universitario y en entidades estatales, las amenazas y riesgos de seguridad de la información son variados:

- **Phishing:** Intentos de engañar a los usuarios para que revelen información sensible. Cuando los cibercriminales hacen phishing envían correos electrónicos fraudulentos que intentan engañar al destinatario para que abra un archivo adjunto cargado de malware o haga clic en un enlace malicioso, la gran diferencia con el smishing es que este envía solo mensajes de texto en lugar de correo electrónico. (Blog Karspesky 2020).
- **Smishing:** El Smishing se define como un mensaje de texto malintencionado que puede estar dirigiéndose a un Smartphone, puede originarse realizando una suplantación del remitente a fin de engañar a quien lo recibe por cuanto este cree que dicho mensaje es de un origen legal y confiable, como es el caso de hacerse pasar por un banco que requiere datos o información personal del usuario engañado quien de esta manera proporciona información financiera.
- **Vishing:** es un tipo de estafa informática parecida al Phishing en el que el ciberdelincuente, valiéndose de la telefonía o el correo electrónico, se hace pasar por una fuente fiable y alegando supuestas razones de seguridad, intenta engañar a sus víctimas para hacerse con sus datos personales. La finalidad que persigue es robar la identidad o bien hacerse con la información bancaria.

- **Ransomware:** Este tipo de amenaza tiene como fin engañarlo mediante una intimidación para que el usuario crea que en alguno de sus dispositivos ha sido hackeado y a su vez le dan la oportunidad de que mediante el pago de alguna suma le ayudan a rescatar su dispositivo de la vulneración realizada, para lo cual le dan un tiempo para hacer efectiva esta solicitud que hacen los mismos ciberdelincuentes, a lo cual aducen ser de ayuda de ingeniería social. El consejo para el usuario es que no pague, sino que verifique si existen fundamentos para suponer que ha sido hackeado, es necesario no confundir este tipo de estafa con el RAMSOMWARE en donde si estamos hablando de un secuestro de la información consistente en un Malware que impide a sus usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a sus documentos. Sin embargo, el pago NO le garantiza que los ciberdelincuentes cumplan con lo prometido y UD pierde tanto la información como su dinero. Se sugiere NO realizar ningún pago y haga caso omiso de esta amenaza, de esta manera no se seguirán fomentando este tipo de estafas.
- **Acceso no autorizado:** Personas no autorizadas que obtienen acceso a sistemas y datos sensibles.
- **Pérdida de datos:** Fallos en los sistemas que resultan en la pérdida de información crítica.
- **Ataques de ingeniería social:** Manipulación psicológica para obtener información confidencial.

3. Importancia de la Educación en Seguridad de la Información

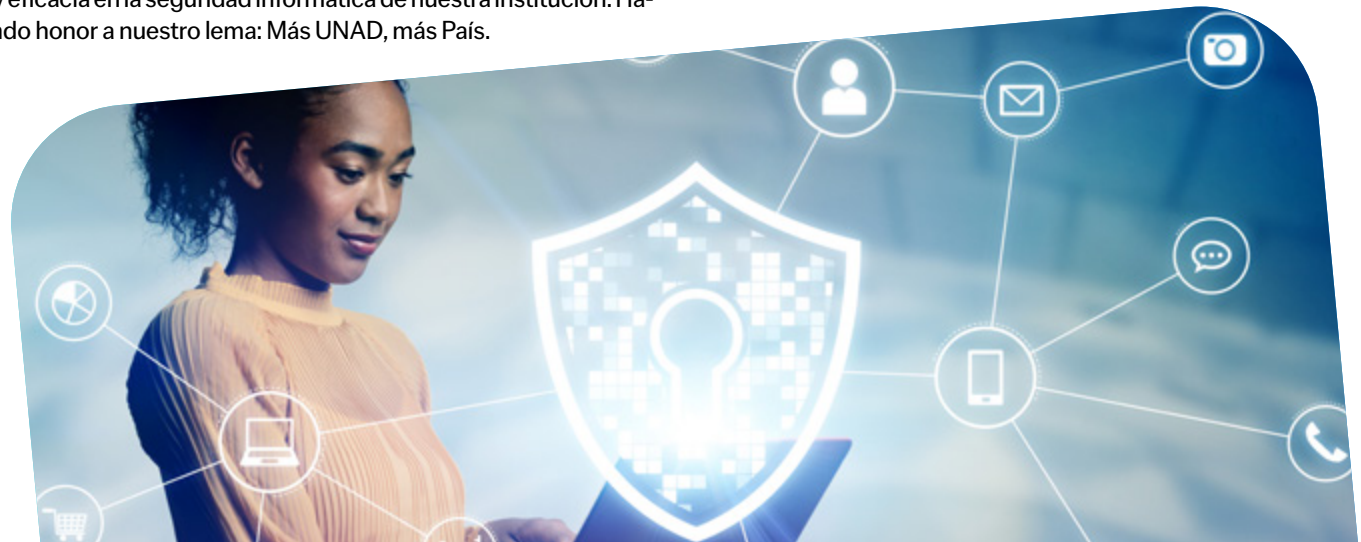
3.1. Concientización y Formación

La educación en seguridad de la información es esencial para mitigar riesgos. La concientización y formación continua ayudan a los usuarios a reconocer y evitar amenazas, reduciendo significativamente la probabilidad de incidentes de seguridad. Programas de capacitación, talleres y campañas de concientización son herramientas efectivas para fortalecer la cultura de seguridad. Así lograremos conformar una red suficientemente informada y actualizada con respecto a las estrategas que nos permitirán una mejor eficiencia y eficacia en la seguridad informática de nuestra institución. Haciendo honor a nuestro lema: Más UNAD, más País.

3.2. Ventajas

Contar con personal preparado en seguridad de la información ofrece múltiples beneficios:

- Reducción de Incidentes: Menos vulnerabilidades explotadas.
- Respuesta Eficiente: Capacidad de responder rápidamente a incidentes de seguridad.
- Mayor Confianza: Mejora la confianza de estudiantes y personal en la protección de sus datos.
- Integridad de los datos.
- Mejora de la imagen corporativa.
- Aumento de la productividad.
- Prevención de gastos imprevistos.
- Mayor capacidad de recuperación y veracidad de los datos.



4. Principios de la Seguridad Informática y Seguridad de la Información Principios Básicos

Figura 1. Pilares de la seguridad

Extraído de Introducción a la seguridad informática y el análisis de vulnerabilidades, Romero et al (2018)

Los principios básicos de seguridad informática y de la información según Romero et al (2018) son:

- **Confidencialidad:** Asegurar que la información solo sea accesible a quienes están autorizados.
- **Integridad:** Mantener la exactitud y completitud de la información y los sistemas. La integridad se refiere a encargarse de proporcionar controles que aseguren que el contenido de dicha información no ha sido modificado y que se mantenga intacta al ser transmitida a otro lugar. Si la integridad no existiera, la información sería manipulada a conveniencia de cualquier persona.
- **Disponibilidad:** Garantizar que la información y los sistemas estén disponibles cuando se necesiten.

4.1. Integración en la cultura organizativa

Para integrar estos principios en la cultura organizativa de la UNAD, se recomienda:

- **Formación Continua:** Implementar programas de capacitación en seguridad de la información.
- **Políticas Claras:** Establecer y comunicar políticas de seguridad claras y comprensibles.
- **Fomento de la Denuncia:** Crear un entorno en el que los miembros de la comunidad se sientan cómodos reportando incidentes de seguridad.

5. Marco legal y normatividad

- Ley 87 de 1993 “Control Interno en los organismos del estado” (Colombia, 1993).
- Ley 527 de 1999 “Comercio Electrónico” (Colombia, Ley 527 de 1999, 2019).
- Ley 594 de 2000 “Ley general de archivo” (Colombia, Ley 594 de 2000, 2000).
- Ley 599 de 2000 “Código penal colombiano” (Senado, Ley 599 de 2000, 2019).
- Ley 603 de 2000 “Control de legalidad del software” (Colombia, Ley 603 de 2000, 2000).
- Ley 734 de 2002 “Código disciplinario único” (Colombia, Ley 734 de 2002, 2002).
- Ley 1266 de 2008 “Por la cual se dictan las disposiciones generales del Habeas Data y se regula el manejo de la información” (Colombia, Ley 1266 de 2008, 2019).
- Ley 1273 de 2009 “Protección de información y de los datos” (Senado, Ley 1273 de 2009, 2019).
- Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales” y su decreto reglamentario 1377 del 27 de junio 2013. (Colombia, Ley 1581 de 2012, 2019).

6. Canales de Comunicación

Grupo de Seguridad de la Información:
Correo electrónico: seguridad.informatica@unad.edu.co
Teléfono: +57 3443700 Ext 1687
Micrositio web: https://gpit.unad.edu.co/seguridad-de-la-informacion

7. Recomendaciones

Para mantener la seguridad de la información, se recomienda a todos los miembros de la comunidad unadista:

- **Participar en Programas de Formación:** Asistir a talleres y cursos de seguridad de la información.
- **Aplicar Buenas Prácticas:** Seguir las directrices establecidas en la cartilla de seguridad de la información.
- **Reportar Incidentes:** Informar de cualquier actividad sospechosa o incidentes de seguridad al grupo de seguridad de la información.

¡Tu colaboración es vital para mantener segura nuestra información! Si observas algo inusual o tienes preguntas sobre seguridad informática, no dudes en comunicarte con nosotros. Juntos, podemos proteger nuestros activos digitales y mantener un entorno seguro para todos en la UNAD!

8. Referencias

1. Romero, I; Figueroa, G, L; Vera, D; Alava, J; Murillo, A; & Castillo, M. (2018) Introducción a la seguridad informática y el Análisis de vulnerabilidades. 3 ciencias-Editorial área de innovación y Desarrollo. S. L recuperado: https://issuu.com/3ciencias/docs/seguridad_inform_tica?utm_medium=referral&utm_source=3ciencias.com
2. Seguridad informática. (2017) Cap 1. Conceptos básicos recuperado de: http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/jerez_l_ca/capitulo1.pdf
3. Seguridad informática (2018). Conceptos básicos. Recuperado de: www.ptolomeo.Unam.mx8080/xmlui/bitstream/handle/132.248.52.100/775/A4.pdf?secuence=4
4. Seguridad informática (2017). Definicion de seguridad. Recuperado de: https://bachilleresrdjimdo.com//app/download/../Seguridad+informática.pdf?