Guía para la Clasificación de los Activos de Información UNADISTAS

Modelo de Seguridad y Privacidad de la Información

Universidad Nacional Abierta y a Distancia
Centro de Respuestas a Incidentes Informáticos

Universidad Nacional Abierta y a Distancia (UNAD)

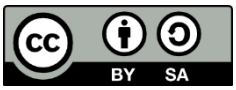
Vicerrectoría de Innovación y Emprendimiento - VIEM
Ing. Andrés Ernesto Salinas
Vicerrector

Escuela de Ciencias Básicas Tecnología e Ingeniería - ECBTI
Ing. Claudio Camilo González Clavijo
Decano

Modelo de Seguridad y Privacidad de la Información UNADISTA

Especialización en Seguridad Informática - ESI
Ing. Sonia Ximena Moreno Molano
Líder de Programa

Grupo de Byte InDesign
Semillero de Investigación Ceros y Unos



Gerencia de Plataformas e Infraestructura Tecnológica

Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD
Luis Fernando Zambrano Hernández
Director

John Fredy Quintero Tamayo
Analista 1

Hernando Peña Hidalgo
Analista 2

Néstor Raúl Cárdenas
Analista 3

Universidad Nacional Abierta y a Distancia
Calle 14 sur No. 14-23 |Bogotá D.C
Correo electrónico: csirt@unad.edu.co
Página web: https://csirt.unad.edu.co

Versión	Observaciones
Versión 1.1 - 13/10/2023	Guía para la Clasificación de los Activos de Información UNADISTAS

Modelo de Seguridad y Privacidad de la Información – MSPI
Universidad Nacional Abierta y a Distancia – UNAD
Vicerrectoría de Innovación y Emprendimiento
Centro de Respuestas a Incidentes Informáticos – CSIRT Académico UNAD

Contenido

Marco Legal y Normatividad 5
Marco Legal 5
Objetivo: 6
Alcance: 6
Definiciones 7
Metodología 9
Clasificación de los Activos de Información 10
Identificación de los Roles y las Responsabilidades del propietario y custodio del activo de información 10
Identificación de activos de información 13
Conclusiones 15
Bibliografía Consultada 16
Anexo 1. Relación entre tipo de activo de información, amenazas e impacto a partir de las dimensiones de la seguridad de la información 17

Marco Legal y Normatividad

Para la construcción del marco de juicio y legal del Modelo de Seguridad y Privacidad UNADSITA, se tiene presente:

Marco Legal

Tabla 1: Normatividad que se debe tener presente para la implementación del MSPI en la UNAD

Constitución Política de Colombia: Artículos 15, 209 y 269	
Leyes	
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales (Congreso de Colombia, 2012)
Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. (Congreso de la Republica, 2014)
CONPES 3854 de 2016	Política Nacional de Seguridad digital
Modelo de Seguridad y Privacidad de la Información - MSPI (MinTIC, 2021)	
Guía 4 (MinTIC, 2016)	
Guía 7 (MinTIC, 2016)	
Guía 21 (MinTIC, 2016)	

Objetivo:

Determinar los lineamientos para clasificar los activos de información en función de su importancia y valor de la Universidad Nacional Abierta y a Distancia UNAD teniendo presente las dimensiones de la seguridad de la información con el fin establecer medidas para la protección adecuada de estos.

Alcance:

Aplica para todos los funcionarios que gestionen y administren información institucional, iniciando con la identificación y catalogación de activos de información teniendo presente normatividad legal y jurídica.

Definiciones[1]

ACTIVO: Cualquier cosa que tiene valor para una organización.

ACTIVO DE INFORMACIÓN: Es el elemento de información que se recibe o produce en el ejercicio de sus funciones. Incluye la información que se encuentre en forma impresa, escrita, en papel, trasmitida por cualquier medio electrónico o almacenado en equipos de cómputo, incluyendo software, hardware, recurso humano, datos contenidos en registros, archivos, bases de datos, videos e imágenes.

En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta que tenga valor para la entidad, por ejemplo: archivos, bases de datos, expedientes, entre otros.

APETITO POR EL RIESGO: El apetito al riesgo establece el contexto aceptable en el que la organización va a planear la estrategia corporativa, sirve como parámetro para la gestión de riesgos e incluye la actitud de la organización respecto al riesgo.[2]

CONFIDENCIALIDAD: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

CUSTODIO: Identifica la parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación de privilegios de acceso, modificación y borrado.

DISPONIBILIDAD: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

INTEGRIDAD: Propiedad de la información relativa a su exactitud y completitud.

INFORMACIÓN: Hace referencia a los datos en formato digital o físico, tratados, creados, procesados, almacenados, archivados o borrados durante la ejecución de procesos misionales de la Superintendencia de Industria y Comercio.

En la ley 1712 de 2014 en el artículo 6, la define como: “un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtenga, adquieran, transformen o controlen”.

INFORMACIÓN PÚBLICA CLASIFICADA: Aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o

[1] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos. Bogotá D.C.: ICONTEC, 2013. p. 2 (NTC-ISO/IEC 27001)

[2] https://www2.deloitte.com/content/dam/Deloitte/mx/Documents/risk/2018/3.Apetito-al-Riesgo.pdf

semiprivado de una persona natural o jurídica porque su acceso podrá ser negado o exceptuando siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 6 de la ley 1712 de 2014.

INFORMACIÓN PÚBLICA RESERVADA: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a interés públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la ley 1712 de 2014.

PROPIETARIO DEL ACTIVO DE INFORMACIÓN: Grupo de trabajo, Oficina, Dirección o Delegatura, que tiene como responsabilidad velar por la protección del activo de información. Tiene responsabilidad de controlar la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos.

RESPONSABLE DEL ACTIVO DE INFORMACIÓN: funcionario designado por el Propietario de Activo de Información para que asuma la responsabilidad de salvaguardarlo.

USUARIO: Todo servidor público, contratista, ente regulador, socio de negocios, tercero, entre otros, que haga uso del activo de información.

TABLA DE RETENCIÓN DOCUMENTAL - TRD: Es un conjunto de unidades documentales homogéneas emanadas por un mismo órgano o sujeto productor en ejercicio de sus funciones ejemplo: contratos, historias laborales, actas.

Metodología

Como apoyo metodológico para la aplicación de esta guía, se hace uso de la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - MAGERIT (España, 2013), aplicando la técnica especifica de uso de tablas para la obtención de resultados.

A continuación, se presentan las escalas definidas para el análisis mediante tablas, "siendo la escala siguiente útil para calificar el valor de los activos, la magnitud del impacto y la magnitud del riesgo". Ver matriz de análisis de riesgos, Hoja METD

Probabilidad del Riesgo

Nomenclatura	Categoría	Valoración
A	Probable	4
M	Posible	3
B	Poco probable	2
MB	muy raro	1

Impacto del Riesgo

Nomenclatura	Categoría	Valoración
A	Alto	4
M	Medio	3
B	Bajo	2
MB	Muy Bajo	1

Estimación del Impacto

MAPA DE CALOR

IMPACTO						
	MA					
	M					
	B					
	MB					
RIESGO		MB	B	M	A	MA
		PROBABILIDAD				

Valoración del Riesgo

Nomenclatura	Categoría	Valoración
MA	Critico	21 25
A	Importante	16 a 20
M	Apreciable	10 a 15
B	Bajo	5 a 9
MB	Despreciable	1 a 4

La metodología MAGERIT plantea un trabajo estructurado para el análisis y la gestión de riesgos de los sistemas de información, ya que se enfoca en el ciclo de vida completo de un sistema de información, teniendo presente la planificación el diseño, la operación y el mantenimiento del análisis de riesgos. Esta metodología tiene como objetivo orientar la identificación y evaluación de los riesgos de seguridad asociados con los sistemas de información, con el fin de establecer medidas de seguridad adecuadas que permitan minimizar los riesgos.

Clasificación de los Activos de Información

Se requiere la identificación y análisis de la siguiente información:

La siguiente tabla, presenta un ejemplo de como se puede abordar la identificación de la información inicial para dar inicio a la catalogación de activos de información.

Tabla 2: Ejemplo de información inicial para la identificación de activos de información.

Razón Social:	Universidad Nacional Abierta y a Distancia - UNAD
Dirección:	Calle 14 Sur # 14 - 23, Bogotá
Persona Contacto:	Gerencia de Plataformas e Infraestructura Tecnológica - GPIT
Actividad Comercial	Educación
Marcos de Trabajo	NTC ISO/IEC 27001 - NTC ISO/IEC 27005 - NTC ISO/IEC 31000
Metodología	El enfoque de gestión de riesgos a aplicar está basado en la metodología MAGERIT

Elaboración propia

La tabla anterior sirve como insumo para reconocer el quehacer de la organización y el marco normativo con el que se ampara la clasificación y catalogación de activos.

Identificación de los Roles y las Responsabilidades del propietario y custodio del activo de información

El artículo 50 de la RESOLUCIÓN No. 007298 DE 10 DE MAYO DE 2023, define: *"**Responsable del activo de información**. Son actores del metasistema Unadista y propietarios de los activos de información delegados por la unidad interesada, los encargados de gestionar y tratar los datos para garantizar su integridad, confidencialidad y disponibilidad que se encuentran en los sistemas de información y bases de datos físicas y digitales de la UNAD, siendo sujetos de control y seguimiento por parte de la GPIT todas las descargas o almacenamientos locales o remotos de información propietaria de la institución, así como su destinación"* (UNAD, 2023). A partir de lo anterior y con relación para la identificación y catalogación de activos de información, se pueden establecer los siguientes roles y responsabilidades[3]:

Tabla 3: Propuesta de roles que pueden intervenir en la identificación y catalogación de activos de información

Rol	Responsabilidad
Propietario del activo de información	Identificar de forma clara qué información es considerada un activo debe establecer una clasificación y valoración de la información que trata. Proteger la información contra accesos no autorizados, modificaciones no autorizadas, divulgación no autorizada y destrucción no autorizada.

[3] https://gobiernodigital.mintic.gov.co/692/articles-5482_G4_Roles_responsabilidades.pdf

	Asignar roles y responsabilidades claras a las personas que tienen acceso a la información, teniendo presente que la responsabilidad sigue siendo del propietario. Monitorear y evaluar el uso de la información para garantizar que se utilice de acuerdo con las políticas de seguridad establecidas. Actualizar y mantener la información para garantizar que sea precisa y esté actualizada. Informar al Centro de Respuestas a incidentes informáticos – CSIRT Académico UNAD a través de los canales de comunicación establecidos de cualquier evento o incidente de ciberseguridad que pueda afectar a la información.
Responsable del Activo de Información	Proteger y preservar la confidencialidad, integridad y disponibilidad del activo de información bajo su responsabilidad. Esto puede incluir el establecimiento y mantenimiento de controles de seguridad apropiados, como políticas, procedimientos y sistemas de seguridad. Identificar los posibles riesgos y vulnerabilidades asociados con dicho activo. Esto implica realizar evaluaciones de riesgos periódicas y utilizar herramientas y técnicas adecuadas para identificar y comprender las posibles amenazas. Implementar y mantener las medidas de seguridad necesarias para proteger el activo de información. Esto puede incluir la implementación de controles técnicos, como firewalls, cifrado de datos, sistemas de detección de intrusos, así como controles físicos y organizativos. Asegurarse de que las políticas y procedimientos de seguridad de la organización se cumplan en relación con el activo de información bajo su responsabilidad. Esto puede implicar la realización de auditorías internas, revisiones de cumplimiento y seguimiento del uso adecuado de los recursos. Actuar de manera oportuna y eficaz para contener, mitigar y resolver la situación. Esto puede implicar la implementación de planes de respuesta a incidentes, la coordinación con otros equipos y la participación en investigaciones de seguridad.

	Mantenerse informado sobre las últimas tendencias, tecnologías y mejores prácticas en materia de seguridad de la información. Esto implica el desarrollo profesional continuo, la participación en capacitaciones y la investigación de nuevas soluciones y enfoques de seguridad.
Custodio	Salvaguardar la información que le ha sido confiada y protegerla contra cualquier acceso no autorizado, modificaciones no autorizadas, divulgación no autorizada y destrucción no autorizada. Implementar en conjunto con el oficial de seguridad las medidas de seguridad necesarias para proteger el activo de información de acuerdo con las políticas y estándares de seguridad de la organización. Monitorear el acceso a la información y garantizar que se utilice de acuerdo con las políticas y estándares de seguridad establecidos. Informar al Centro de Respuestas a incidentes informáticos – CSIRT Académico UNAD a través de los canales de comunicación establecidos de cualquier evento o incidente de ciberseguridad que pueda afectar a la información. Mantener registros precisos y actualizados del acceso y uso del activo de información. Capacitar a los usuarios sobre las políticas y estándares de seguridad de la organización para garantizar que se utilice el activo de información de manera segura y responsable. Proporcionar informes regulares sobre la seguridad del activo de información a la dirección y otros interesados pertinentes. Asignar los accesos y privilegios de uso al activo de información. Realizar copia de información del activo de información. Modificar o aplicar controles de seguridad al activo de información. Eliminar o destruir el activo de información. Realizar el borrado seguro de la información que gestione o trate el activo de información

Elaboración propia

En la Universidad Nacional Abierta y a Distancia UNAD, la Gerencia de Plataformas e infraestructura Tecnológica - GPIT y la Unidad responsable del activo deben establecer y mantener políticas de seguridad para la protección adecuada de la información. Esto incluye la implementación de medidas de seguridad físicas y lógicas para la protección de la información. En este sentido, la información mínima requerida para identificar el propietario, responsable o custodios de la información UNADISTA puede ser:

Tabla 4: Información mínima requerida para la identificación de personas que intervienen en la administración, protección y custodia de la información que gestiona un activo de información.

	Datos
Nombres completos	
Unidad a la que pertenece	
Funciones y responsabilidades	
Correo institucional	
Teléfono de Contacto	
Tipo de rol	Propietario: ☐ Custodio: ☐ Responsable: ☐

Elaboración propia

Los roles y responsabilidades para salvaguardar la ciberseguridad de la Universidad se encuentran planteados en la Guía de Roles y Responsabilidades de la seguridad de la información UNADISTA.

Identificación de activos de información

Una propuesta para la identificación de los activos de información de la Universidad Nacional Abierta y a Distancia (UNAD, 2023) es la que se presenta en la siguiente tabla, la cual puede contener información que se orienta a partir de establecido por la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información MAGERIT

Tabla 5: Ejemplo de información que sierve como insumo para la identificación de un activo de información

Nombre del activo de información	Indicar el nombre del activo de información
Descripción	Indicar de forma clara cuál es el objetivo del activo de información
Cantidad	Indicar la cantidad de activos de información de este tipo
Tipo de activo de información	Indicar el tipo de activo de información teniendo como referencia el anexo 1 de este documento
Especificación Según MAGERIT	Detallar a partir de la metodología el tipo de activo de información teniendo como referencia el anexo 1 de este documento
Proceso al que pertenece	Indicar a que proceso del SIG pertenece el activo de información

Propietario del activo de información	Indicar la Unidad a la cual tiene como responsabilidad la gestiona el activo de información
Responsable del activo de información	Indicar el nombre completo del funcionario o externo el cual es responsable del activo de información
Custodio del activo de información	Indicar Unidad responsable de la custodia del activo de información
Dueño del dato	Indicar quien es el dueño del dato (Aspirante, estudiante, egresado, funcionario, otro)
Tipo de información que gestiona	Teniendo presente la ley 1712 de 2014, indicar si la información es publica o reservada[4]
Tipo de datos que contiene	Teniendo presente la ley 1581 de 2012 indicar si el activo de información contiene datos públicos, privados, semiprivados o sensibles o datos personales o no personales[5]
Requiere registrar ante el RNBD	Indicar si la información que contiene el activo este o debe estar reportada en el RNBD[6]
Ubicación del activo	Indicar la ubicación del activo de información determinando si es Física o Digital

Elaboración propia

Una vez identificado el activo de información, se podrían plantear algunas preguntas orientadoras las cuales permiten reconocer un poco más la importancia del activo de información en términos de protección a terceros, exposición del activo, la restricción a un número limitado de funcionarios, la criticidad del activo respecto a las operaciones de la Universidad, entre otros. La siguiente tabla platea varios interrogantes que pueden ser plateados:

Tabla 6: Interrogantes propuestos para el reconocimiento de un activo de información

¿El activo de información debe protegerse de terceros o de partes interesadas?	SI ☐ NO ☐
¿Es un activo que se encuentra expuesto en internet?	SI ☐ NO ☐
¿El activo se debe restringir a un número limitado de funcionarios?	SI ☐ NO ☐
¿El activo debe ser restringido a personas externas?	SI ☐ NO ☐
¿El activo se puede alter o comprometer para fraudes o corrupción?	SI ☐ NO ☐
¿El activo es crítico para las operaciones de la Universidad?	SI ☐ NO ☐
¿El activo es crítico respecto al servicio hacia terceros?	SI ☐ NO ☐

[4] https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882
[5] https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981
[6] https://www.sic.gov.co/registro-nacional-de-bases-de-datos

Activo de información que, en caso de ser conocido, utilizado o modificado por alguna persona o sistema sin la debida autorización, impactaría negativamente a los sistemas y/o procesos de la empresa, de manera:	Leve ☐ Importante ☐ Grave ☐

Recuperado de Matriz de Análisis de riesgos propuesta por estudiantes del curso de Administración y Gestión del Riesgo del programa de Especialización en Seguridad Informática de la UNAD

Conclusiones

Identificar y catalogar los activos de información de una organización es fundamental para reconocer cuales son los activos de información que son de importancia para la institución y que pueden presentar impacto en el momento de presentarse un evento o incidente informático. A partir de lo anterior es preciso tener en cuenta:

La norma ISO/IEC 27001:2022 establece que la identificación y catalogación de activos de información son pasos esenciales en el proceso de gestión de la seguridad de la información, al realizar este proceso, la Universidad se aseguran de cumplir con estándares de seguridad de la información propuestos en el orden mundial.

La metodología MAGERIT, instrumento que brinda orientación y ampliamente aplicado en organizaciones publico privadas, se basa en la gestión de riesgos de seguridad de la información. En este sentido, la identificación de activos de información es el punto de partida para evaluar y gestionar los riesgos asociados a los activos de información identificados.

Al catalogar los activos de información, la Institución empieza a identificar cuáles de estos se presentan como más críticos respecto a la ejecución de sus operaciones, lo cual facilita la asignación de recursos y medidas de seguridad específicas para proteger esos activos, reduciendo así el impacto de posibles incidentes.

Respecto al cumplimiento legal y normativo Colombiano, el modelo de seguridad de la privacidad de la información MSPI establece requisitos específicos para proteger la privacidad de los datos. A partir de esto, identificar y catalogar los activos de información ayuda a garantizar el cumplimiento de regulaciones, evitando sanciones y riesgos legales.

La identificación y catalogación de activos de información no es un proceso estático, se debe ver como un componente clave de la mejora continua en la gestión de la seguridad de la información UNADISTA, contribuyendo así en contemplar estrategias de seguridad a medida que evolucionan los activos y las amenazas, manteniendo la protección de la información actualizada y efectiva.

Bibliografía Consultada

Congreso de Colombia. (2012). Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Congreso de la Republica. (2014). Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882

España, G. d. (2013). Obtenido de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

MinTIC. (2016). *Guia de Gestión de Riesgos*. Obtenido de https://gobiernodigital.mintic.gov.co/692/articles-5482_G7_Gestion_Riesgos.pdf

MinTIC. (2016). *Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.* Obtenido de https://gobiernodigital.mintic.gov.co/692/articles-5482_G21_Gestion_Incidentes.pdf

MinTIC. (2016). *Roles y Responsabilidades.*

MinTIC. (2016). *Roles y Responsabilidades.* Obtenido de https://gobiernodigital.mintic.gov.co/692/articles-5482_G4_Roles_responsabilidades.pdf

MinTIC. (2021). *Anexo 1 Modelo se Seguridad y Privacidad de la Información.*

UNAD. (2023). Obtenido de https://csirt.unad.edu.co/images/2023/Publicaciones/Resolucion%20SGSI%20VRF.pdf

UNAD, C. A. (2023). Obtenido de https://selloeditorial.unad.edu.co/images/2022/boletines-cip-csirt/Boletin_13.pdf

Anexo 1. Relación entre tipo de activo de información, amenazas e impacto a partir de las dimensiones de la seguridad de la información[7]

Tipo de Activo	Descripción	Ejemplos
[D] Datos - Información	Se relaciona con la información que es gestionada y tratada a través de los sistemas de información y su talento humano	[files] ficheros [backup] copias de respaldo [conf] datos de configuración [int] datos de gestión interna [password] credenciales [auth] datos de validación de credenciales [acl] datos de control de acceso [log] registros de actividad [source] código fuente [exe] código ejecutable [test] datos de prueba

Los activos de información tipo [D] Dato, pueden estar expuestos a las siguientes amenazas e impactan de forma directa a las dimensiones de seguridad con las que se encuentran relacionadas[8]

Amenaza	Dimensiones de la Información				
[E1] Errores de los usuarios	[D]	[C]	[I]		
[E2] Errores del administrador	[D]	[C]	[I]		
[E3] Errores de monitorización (log)			[I]	[T]	
[E4] Errores de configuración			[I]		
[E15] Alteración accidental de la información			[I]		
[E18] Destrucción de información	[D]				
[E19] Fugas de información		[C]			
[A3] Manipulación de los registros de actividad (log)			[I]	[T]	
[A4] Manipulación de la configuración		[C]	[I]		[A]
[A5] Suplantación de la identidad del usuario		[C]	[I]		[A]
[A6] Abuso de privilegios de acceso	[D]	[C]	[I]		
[A11] Acceso no autorizado		[C]	[I]		
[A13] Repudio			[I]	[T]	
[A15] Modificación deliberada de la información			[I]		
[A18] Destrucción de información	[D]				
[A19] Divulgación de información		[C]			

[7] https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Tipo de Activo	Descripción	Ejemplos
[K] Claves criptográficas	Hace referencia a los modelos que se usan para encriptar y proteger la información	[info] protección de la información [encrypt] claves de cifra [shared_secret] secreto compartido (clave simétrica) [public_encryption] clave pública de cifra [public_decryption] clave privada de descifrado [sign] claves de firma [shared_secret] secreto compartido (clave simétrica) [public_signature] clave privada de firma (2) [public_verification] clave pública de verificación de firma (2) [com] protección de las comunicaciones [channel] claves de cifrado del canal [authentication] claves de autenticación [verification] claves de verificación de autenticación [disk] cifrado de soportes de información [encrypt] claves de cifra [x509] certificados de clave pública

Los activos de información tipo [K] Claves criptográficas, pueden estar expuestos a las siguientes amenazas e impactan de forma directa a las dimensiones de seguridad con las que se encuentran relacionadas[9]

AMENAZA	Dimensiones de la seguridad de la Información				
[E1] Errores de los usuarios	[D]	[C]	[I]		
[E2] Errores del administrador	[D]	[C]	[I]		
[E15] Alteración accidental de la información			[I]		
[E18] Destrucción de información	[D]				
[E19] Fugas de información		[C]			
[A5] Suplantación de la identidad del usuario		[C]	[I]		[A]
[A6] Abuso de privilegios de acceso	[D]	[C]	[I]		
[A11] Acceso no autorizado		[C]	[I]		
[A15] Modificación deliberada de la información			[I]		
[A18] Destrucción de información	[D]				
[A19] Divulgación de información		[C]			

[9] [D] [D] – [C] [C] – [[I]] – [T] TRAZABAILIDAD – [A] [A]

Tipo de Activo	Descripción	Ejemplos
[S] Servicios	Son los activos que permiten a un usuario dar respuesta a una necesidad en términos de servicio de infraestructura lógica o física	[anon] anónimo (sin requerir identificación del usuario) [pub] al público en general (sin relación contractual) [ext] a usuarios externos (bajo una relación contractual) [int] interno (a usuarios de la propia organización) [www] world wide web [telnet] acceso remoto a cuenta local [email] correo electrónico [file] almacenamiento de ficheros [ftp] transferencia de ficheros [edi] intercambio electrónico de datos [dir] servicio de directorio [idm] gestión de identidades [ipm] gestión de privilegios [pki] PKI - infraestructura de clave pública

AMENAZA	Dimensiones de la Seguridad de la Información				
[E1] Errores de los usuarios	[D]	[C]	[I]		
[E2] Errores del administrador	[D]	[C]	[I]		
[E9] Errores de [re-]encaminamiento		[C]			
[E10] Errores de secuencia			[I]		
[E15] Alteración accidental de la información			[I]		
[E18] Destrucción de información	[D]				
[E19] Fugas de información		[C]			
[E24] Caída del sistema por agotamiento de recursos	[D]				
[A5] Suplantación de la identidad del usuario		[C]	[I]		[A]
[A6] Abuso de privilegios de acceso	[D]	[C]	[I]		
[A7] Uso no previsto	[D]	[C]	[I]		
[A9] [Re-]encaminamiento de mensajes		[C]			
[A10] Alteración de secuencia			[I]		
[A11] Acceso no autorizado		[C]	[I]		
[A13] Repudio			[I]	[T]	
[A15] Modificación deliberada de la información			[I]		
[A18] Destrucción de información	[D]				
[A19] Divulgación de información		[C]			
[A24] Denegación de servicio	[D]				

Tipo de Activo	Descripción	Ejemplos
[SW] Software	Hace referencia a los componentes y programas de software utilizados en una organización	[prp] desarrollo propio (in house) [sub] desarrollo a medida (subcontratado) [std] estándar (off the shelf) [browser] navegador web [www] servidor de presentación [app] servidor de aplicaciones [email_client] cliente de correo electrónico [email_server] servidor de correo electrónico [file] servidor de ficheros [dbms] sistema de gestión de bases de datos [tm] monitor transaccional [office] ofimática [av] anti virus [os] sistema operativo [hypervisor] gestor de máquinas virtuales [ts] servidor de terminales [backup] sistema de backup

AMENAZA	Dimensiones de la Seguridad de la Información				
[I5] Avería de origen físico o lógico	[D]				
[E1] Errores de los usuarios	[D]	[C]	[I]		
[E2] Errores del administrador	[D]	[C]	[I]		
[E8] Difusión de software dañino	[D]	[C]	[I]		
[E9] Errores de [re-]encaminamiento		[C]			
[E10] Errores de secuencia			[I]		
[E15] Alteración accidental de la información			[I]		
[E18] Destrucción de información	[D]				
[E19] Fugas de información		[C]			
[E20] Vulnerabilidades de los programas (software)	[D]	[C]	[I]		
[E21] Errores de mantenimiento / actualización de programas (software)	[D]		[I]		
[A5] Suplantación de la identidad del usuario		[C]	[I]		[A]
[A6] Abuso de privilegios de acceso	[D]	[C]	[I]		
[A7] Uso no previsto	[D]	[C]	[I]		
[A8] Difusión de software dañino	[D]	[C]	[I]		
[A9] [Re-]encaminamiento de mensajes		[C]			
[A10] Alteración de secuencia			[I]		
[A11] Acceso no autorizado		[C]	[I]		
[A15] Modificación deliberada de la información			[I]		
[A18] Destrucción de información	[D]				
[A19] Divulgación de información		[C]			
[A22] Manipulación de programas	[D]	[C]	[I]		

Tipo de Activo	Descripción	Ejemplos según MAGERIT
[HW] Hardware	Hace referencia a los componentes físicos y dispositivos electrónicos que forman parte de la infraestructura tecnológica la universidad	[host] grandes equipos [mid] equipos medios [pc] informática personal [mobile] informática móvil [pda] agendas electrónicas [vhost] equipo virtual [backup] equipamiento de respaldo [peripheral] periféricos [print] medios de impresión [scan] escáneres [crypto] dispositivos criptográficos [bp] dispositivo de frontera [network] soporte de la red [modem] módems [hub] concentradores [switch] conmutadores [router] encaminadores [bridge] pasarelas [firewall] cortafuegos [wap] punto de acceso inalámbrico [pabx] centralita telefónica [ipphone] teléfono IP

AMENAZA	Dimensiones de la Seguridad de la Información				
[N1] Fuego	[D]				
[N2] Daños por agua	[D]				
[N*] Desastres naturales	[D]				
[I1] Fuego	[D]				
[I2] Daños por agua	[D]				
[I*] Desastres industriales	[D]				
[I3] Contaminación mecánica	[D]				
[I4] Contaminación electromagnética	[D]				
[I5] Avería de origen físico o lógico	[D]				
[I6] Corte del suministro eléctrico	[D]				
[I7] Condiciones inadecuadas de temperatura o humedad	[D]				
[I11] Emanaciones electromagnéticas		[C]			
[E2] Errores del administrador	[D]	[C]	[I]		
[E23] Errores de mantenimiento / actualización de equipos (hardware)	[D]				
[E24] Caída del sistema por agotamiento de recursos	[D]				
[E25] Pérdida de equipos	[D]	[C]			
[A6] Abuso de privilegios de acceso	[D]	[C]	[I]		
[A7] Uso no previsto	[D]	[C]	[I]		
[A11] Acceso no autorizado		[C]	[I]		
[A23] Manipulación de los equipos	[D]	[C]			
[A24] Denegación de servicio	[D]				
[A25] Robo	[D]	[C]			
[A26] Ataque destructivo	[D]				

Tipo de Activo	Descripción	Ejemplos
[COM] Redes de comunicación	Hace referencia a los recursos y componentes utilizados para la transmisión y recepción de información dentro de la Universidad	[PSTN] red telefónica [ISDN] rdsi (red digital) [X25] X25 (red de datos) [ADSL] ADSL [pp] punto a punto [radio] comunicaciones radio [wifi] red inalámbrica [mobile] telefonía móvil [sat] por satélite [LAN] red local [MAN] red metropolitana [Internet] Internet

AMENAZA	Dimensiones de la Seguridad de la Información				
[I8] Fallo de servicios de comunicaciones	[D]				
[E2] Errores del administrador	[D]	[C]	[I]		
[E9] Errores de [re-]encaminamiento		[C]			
[E10] Errores de secuencia			[I]		
[E15] Alteración accidental de la información			[I]		
[E18] Destrucción de información	[D]				
[E19] Fugas de información		[C]			
[E24] Caída del sistema por agotamiento de recursos	[D]				
[A5] Suplantación de la identidad del usuario		[C]	[I]		[A]
[A6] Abuso de privilegios de acceso	[D]	[C]	[I]		
[A7] Uso no previsto	[D]	[C]	[I]		
[A9] [Re-]encaminamiento de mensajes		[C]			
[A10] Alteración de secuencia			[I]		
[A11] Acceso no autorizado		[C]	[I]		
[A12] Análisis de tráfico		[C]			
[A14] Interceptación de información (escucha)		[C]			
[A15] Modificación deliberada de la información			[I]		
[A19] Divulgación de información		[C]			
[A24] Denegación de servicio	[D]				

Tipo de Activo	Descripción	Ejemplos
[Media] Soportes de información		[electronic] electrónicos [disk] discos [vdisk] discos virtuales [san] almacenamiento en red [disquette] disquetes [cd] cederrón (CD-ROM) [usb] memorias USB [dvd] DVD [tape] cinta magnética [mc] tarjetas de memoria [ic] tarjetas inteligentes [non_electronic] no electrónicos [printed] material impreso [tape] cinta de papel [film] microfilm [cards] tarjetas perforadas

AMENAZA	Dimensiones de la Seguridad de la Información				
[N1] Fuego	[D]				
[N2] Daños por agua	[D]				
[N*] Desastres naturales	[D]				
[I1] Fuego	[D]				
[I2] Daños por agua	[D]				
[I*] Desastres industriales	[D]				
[I3] Contaminación mecánica	[D]				
[I4] Contaminación electromagnética	[D]				
[I5] Avería de origen físico o lógico	[D]				
[I6] Corte del suministro eléctrico	[D]				
[I7] Condiciones inadecuadas de temperatura o humedad	[D]				
[I10] Degradación de los soportes de almacenamiento de la información	[D]				
[I11] Emanaciones electromagnéticas		[C]			
[E1] Errores de los usuarios	[D]	[C]	[I]		
[E2] Errores del administrador	[D]	[C]	[I]		
[E15] Alteración accidental de la información			[I]		
[E18] Destrucción de información	[D]				
[E19] Fugas de información		[C]			
[E23] Errores de mantenimiento / actualización de equipos (hardware)	[D]				
[E25] Pérdida de equipos	[D]	[C]			
[A7] Uso no previsto	[D]	[C]	[I]		
[A11] Acceso no autorizado		[C]	[I]		
[A15] Modificación deliberada de la información			[I]		
[A18] Destrucción de información	[D]				
[A19] Divulgación de información		[C]			
[A23] Manipulación de los equipos	[D]	[C]			
[A25] Robo	[D]	[C]			
[A26] Ataque destructivo	[D]				

Tipo de Activo	Descripción	Ejemplos
[AUX] Equipamiento auxiliar	Hace referencia aa los elementos y dispositivos que, si bien no son parte central de los sistemas de información, son necesarios para el funcionamiento de los sistemas, los cuales brindan soporte a las operaciones tecnológicas de la Universidad	[power] fuentes de alimentación [ups] sistemas de alimentación ininterrumpida [gen] generadores eléctricos [ac] equipos de climatización [cabling] cableado [wire] cable eléctrico [fiber] fibra óptica [robot] robots [tape] ... de cintas [disk] ... de discos [supply] suministros esenciales [destroy] equipos de destrucción de soportes de información [furniture] mobiliario: armarios, etc [safe] cajas fuertes

AMENAZA	Dimensiones de la Seguridad de la Información				
[N1] Fuego	[D]				
[N2] Daños por agua	[D]				
[N*] Desastres naturales	[D]				
[I1] Fuego	[D]				
[I2] Daños por agua	[D]				
[I*] Desastres industriales	[D]				
[I3] Contaminación mecánica	[D]				
[I4] Contaminación electromagnética	[D]				
[I5] Avería de origen físico o lógico	[D]				
[I6] Corte del suministro eléctrico	[D]				
[I7] Condiciones inadecuadas de temperatura o humedad	[D]				
[I9] Interrupción de otros servicios y suministros esenciales	[D]				
[I11] Emanaciones electromagnéticas		[C]			
[E23] Errores de mantenimiento / actualización de equipos (hardware)	[D]				
[E25] Pérdida de equipos	[D]	[C]			
[A7] Uso no previsto	[D]	[C]	[I]		
[A11] Acceso no autorizado		[C]	[I]		
[A23] Manipulación de los equipos	[D]	[C]			
[A25] Robo	[D]	[C]			
[A26] Ataque destructivo	[D]				

Tipo de Activo	Descripción	Ejemplos
[L] Instalaciones	Hace referencia a los espacios físicos y las estructuras donde se encuentran alojados los sistemas de información y los activos tecnológicos de la Universidad	[site] recinto [building] edificio [local] cuarto [mobile] plataformas móviles [car] vehículo terrestre: coche, camión, etc. [plane] vehículo aéreo: avión, etc. [ship] vehículo marítimo: buque, lancha, etc. [shelter] contenedores [channel] canalización [backup] instalaciones de respaldo

AMENAZA	Dimensiones de la Seguridad de la Información				
[N1] Fuego	[D]				
[N2] Daños por agua	[D]				
[N*] Desastres naturales	[D]				
[I1] Fuego	[D]				
[I2] Daños por agua	[D]				
[I*] Desastres industriales	[D]				
[I11] Emanaciones electromagnéticas		[C]			
[E15] Alteración accidental de la información			[I]		
[E18] Destrucción de información	[D]				
[E19] Fugas de información		[C]			
[A7] Uso no previsto	[D]	[C]	[I]		
[A11] Acceso no autorizado		[C]	[I]		
[A15] Modificación deliberada de la información			[I]		
[A18] Destrucción de información	[D]				
[A19] Divulgación de información		[C]			
[A26] Ataque destructivo	[D]				
[A27] Ocupación enemiga	[D]	[C]			

Tipo de Activo	Descripción	Ejemplos
[P] Personal	Hace referencia al personal de la Universidad que está involucrado en el uso, operación, mantenimiento y gestión de los sistemas de información y la infraestructura tecnológica	[ue] usuarios externos [ui] usuarios internos [op] operadores [adm] administradores de sistemas [com] administradores de comunicaciones [dba] administradores de BBDD [sec] administradores de seguridad [des] desarrolladores / programadores [sub] subcontratas [prov] proveedores

AMENAZA	Dimensiones de la Seguridad de la Información				
[E7] Deficiencias en la organización	[D]				
[E19] Fugas de información		[C]			
[E28] In[D] del personal	[D]				
[A28] In[D] del personal	[D]	[C]			
[A29] Extorsión	[D]	[C]	[I]		
[A30] Ingeniería social (picaresca)	[D]	[C]	[I]		