



UNIVERSIDAD DE
COSTA RICA

Rectoría

Gestión institucional del riesgo y Aplicación en TI

César Picado

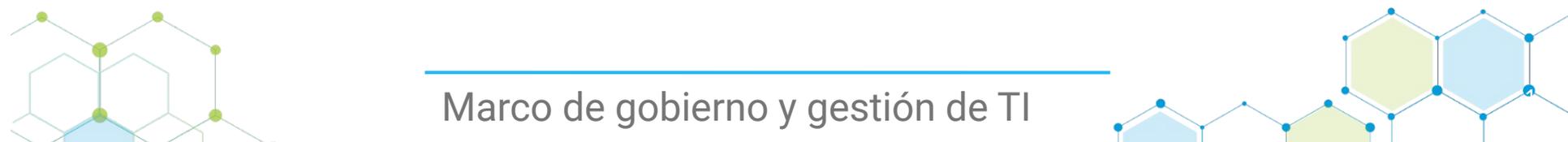
Oficina de Planificación, UCR

Abel Brenes Arce

Centro de Informática, UCR

17 agosto 2022

Marco de gobierno y gestión de TI





Agenda

- Marco normativo y organización
- Sistema de Control Interno
- Gestión Institucional del riesgo
- Comunicación y Ciudadanía digital
- Exposición al Riesgo y escenario de ataques
- Gestión del riesgo y Seguridad TI



UNIVERSIDAD DE
COSTA RICA

Rectoría

Gestión institucional del riesgo y Aplicación en TI

Marco normativo nacional y orientador UCR, control interno, planes y herramientas.





Marco Normativo

COSO (Committee of Sponsoring Organizations of the Treadway Commission)

Ley General de Control Interno No. 8292

Normas de Control Interno para el Sector Público

Directrices del SEVRI

Marco orientador UCR

Ley General de Control Interno No.8292

Artículo 8º-Concepto de sistema de control interno. Para efectos de esta Ley, se entenderá por sistema de control interno la serie de acciones ejecutadas por la administración activa, diseñadas para proporcionar seguridad en la consecución de los siguientes objetivos:

- Proteger y conservar el patrimonio público
- Mantener sistemas de información confiables y oportunos
- Garantizar la eficiencia y eficacia de las operaciones en las instituciones públicas
- Lograr un cumplimiento estricto de la normativa jurídica y técnica vigente

Aspectos de organización

Jerarca: superior jerárquico del órgano o del ente; ejerce la máxima autoridad dentro del órgano o ente, unipersonal o colegiado.

Titular subordinado: funcionario de la administración activa responsable de un proceso, con autoridad para ordenar y tomar decisiones.



Responsabilidades

ARTÍCULO 7.- Obligatoriedad de disponer de un sistema de control interno

Los entes y órganos sujetos a esta Ley dispondrán de sistemas de control interno, los cuales deberán ser aplicables, completos, razonables, integrados y congruentes con sus competencias y atribuciones institucionales. Además, deberán proporcionar seguridad en el cumplimiento de esas atribuciones y competencias; todo conforme al primer párrafo del artículo 3 de la presente Ley.

ARTÍCULO 10.- Responsabilidad por el sistema de control interno

Serán responsabilidad del jerarca y del titular subordinado establecer, mantener, perfeccionar y evaluar el sistema de control interno institucional. Asimismo, será responsabilidad de la administración activa realizar las acciones necesarias para garantizar su efectivo funcionamiento.

Aspectos de organización

Proceso de Control y Fiscalización

- Se orienta a garantizar la legalidad y eficiencia de los controles internos y del manejo de los fondos públicos



Aspectos de organización

- Jerarca y titular subordinado
- Cada unidad ejecutora
- OPLAU (coordinador, facilitador)
- Contraloría interna (fiscalizador)



¿Qué es control?

Es el proceso de determinar lo que se está llevando a cabo y compararlo con el cómo DEBE llevarse a cabo

¿Para qué el control interno?

Para determinar desviaciones y establecer las medidas necesarias a fin de evitar situaciones que pongan en peligro la legalidad, eficiencia y eficacia de los objetivos y metas institucionales.

Beneficios del Control Interno

Permite identificar oportunidades de mejora en los procesos.

Logra la detección y atención oportuna de situaciones que puedan alejar a la unidad y a la Institución del logro de sus objetivos.

Facilita la transparencia y rendición de cuentas.

Protección de los recursos de la Institución.

Mejora la gestión de la información.

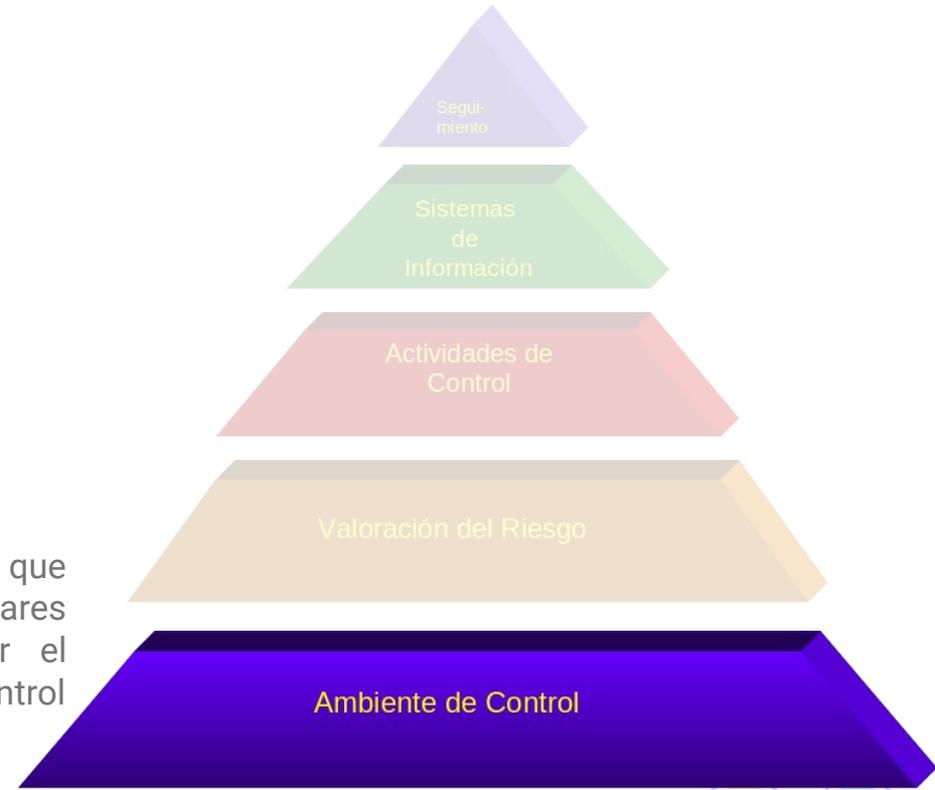
Brinda garantía razonable del logro de los objetivos y metas.

Componentes funcionales del Sistema de Control Interno



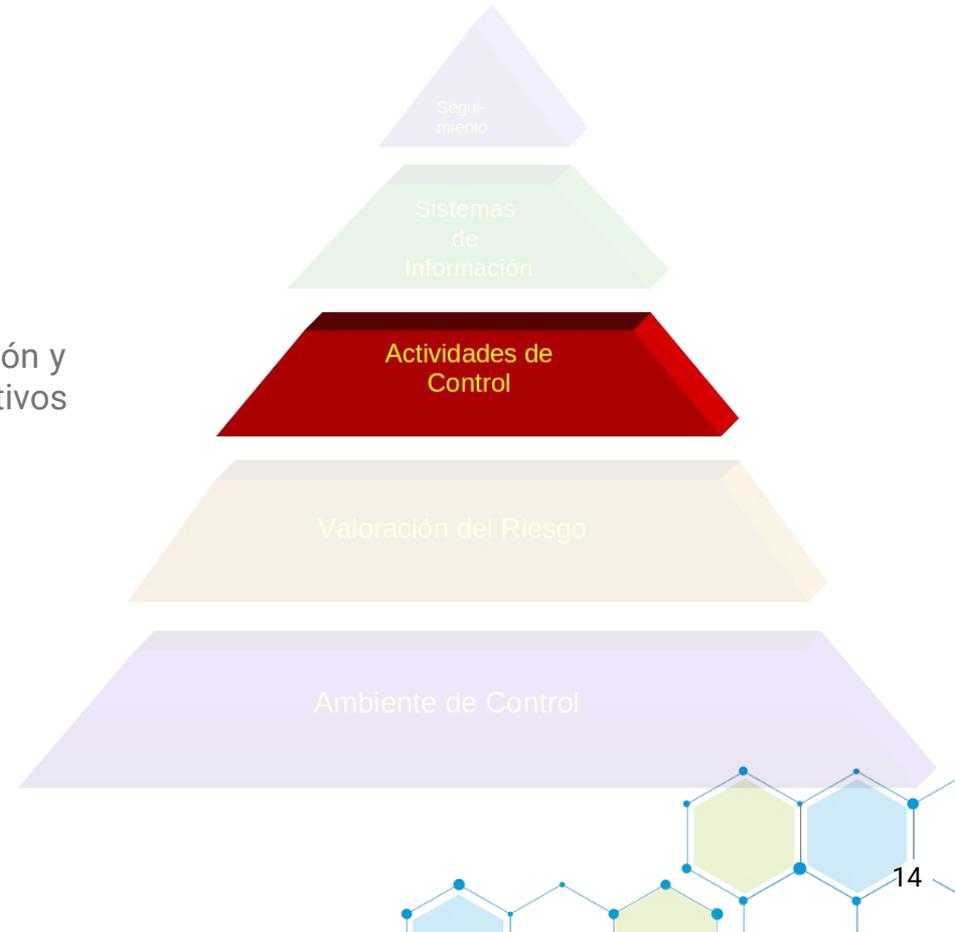
Componentes funcionales del Sistema de Control Interno

El conjunto de factores del ambiente organizacional que deben establecer y mantener el jerarca, los titulares subordinados y demás funcionarios, para permitir el desarrollo de una actitud positiva y de apoyo para el control interno y para una administración escrupulosa.



Componentes funcionales del Sistema de Control Interno

Políticas y procedimientos que contribuyen a la operación y el fortalecimiento del SCI y el logro de los objetivos institucionales.



Componentes funcionales del Sistema de Control Interno

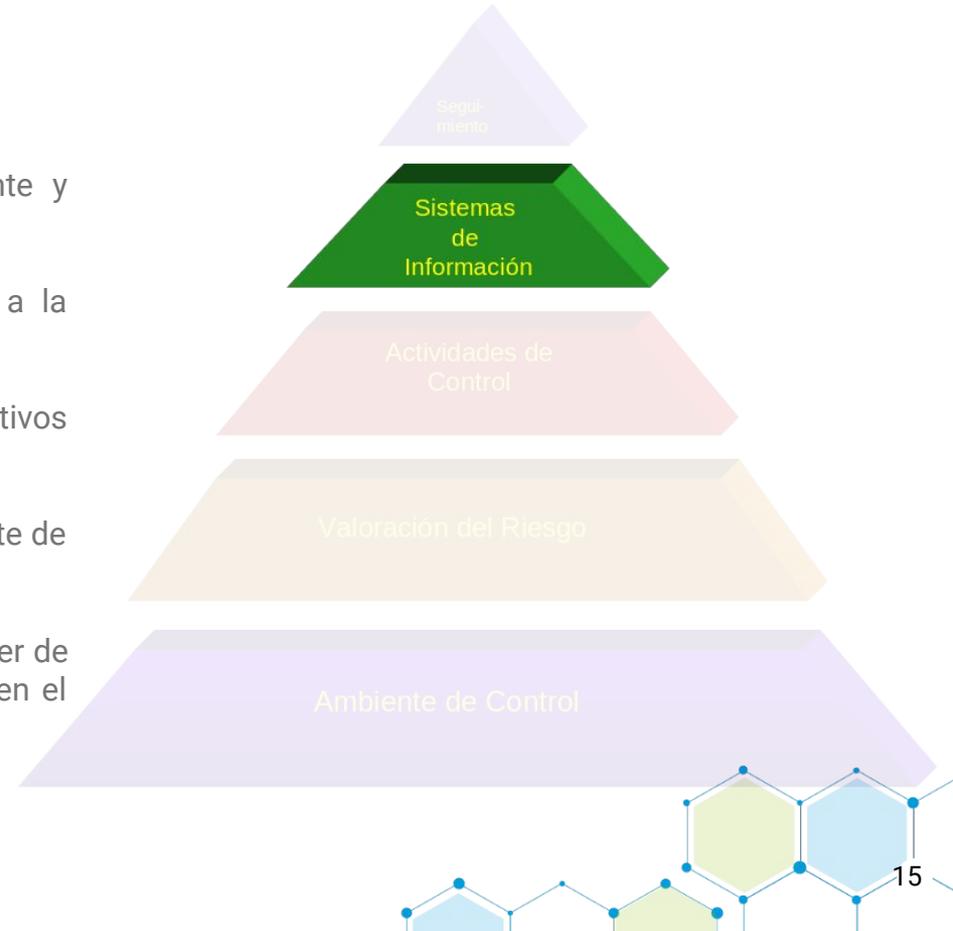
La información debe ser confiable, relevante, pertinente y oportuna.

Deben asegurarse que la información sea comunicada a la persona que la necesite de forma eficiente y eficaz.

Alinear los sistemas de información con los objetivos institucionales.

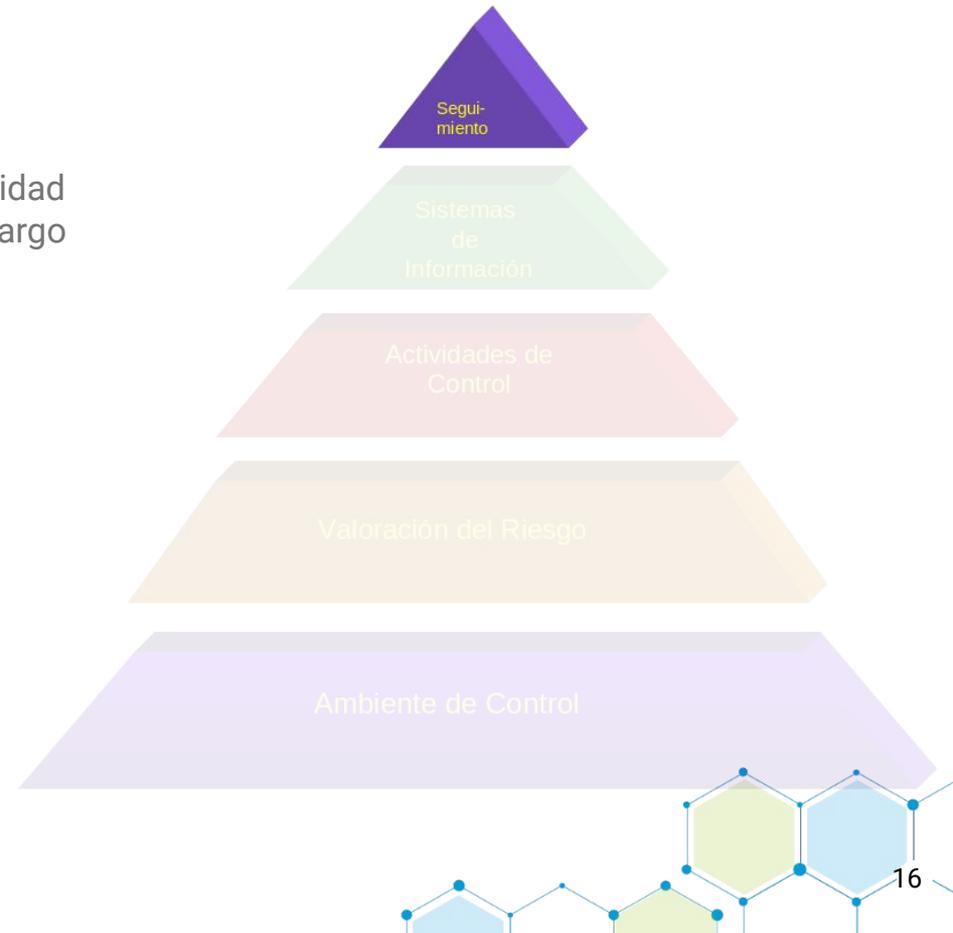
Verificar que sean adecuados para el cuidado y manejo eficiente de los recursos públicos.

Establecer políticas, procedimientos y recursos para disponer de un archivo institucional, de conformidad con lo señalado en el ordenamiento jurídico y técnico.



Componentes funcionales del Sistema de Control Interno

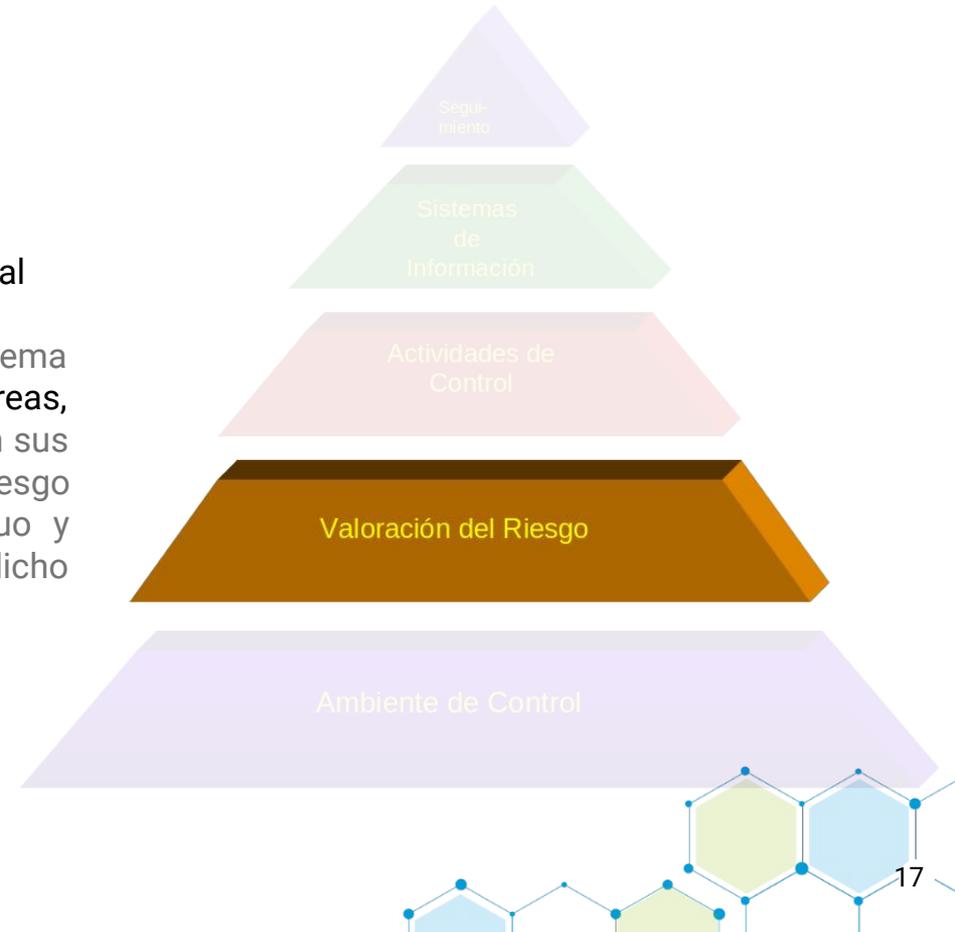
Son las actividades que se realizan para valorar la calidad del funcionamiento del sistema de control interno, a lo largo del tiempo.



Componentes funcionales del Sistema de Control Interno

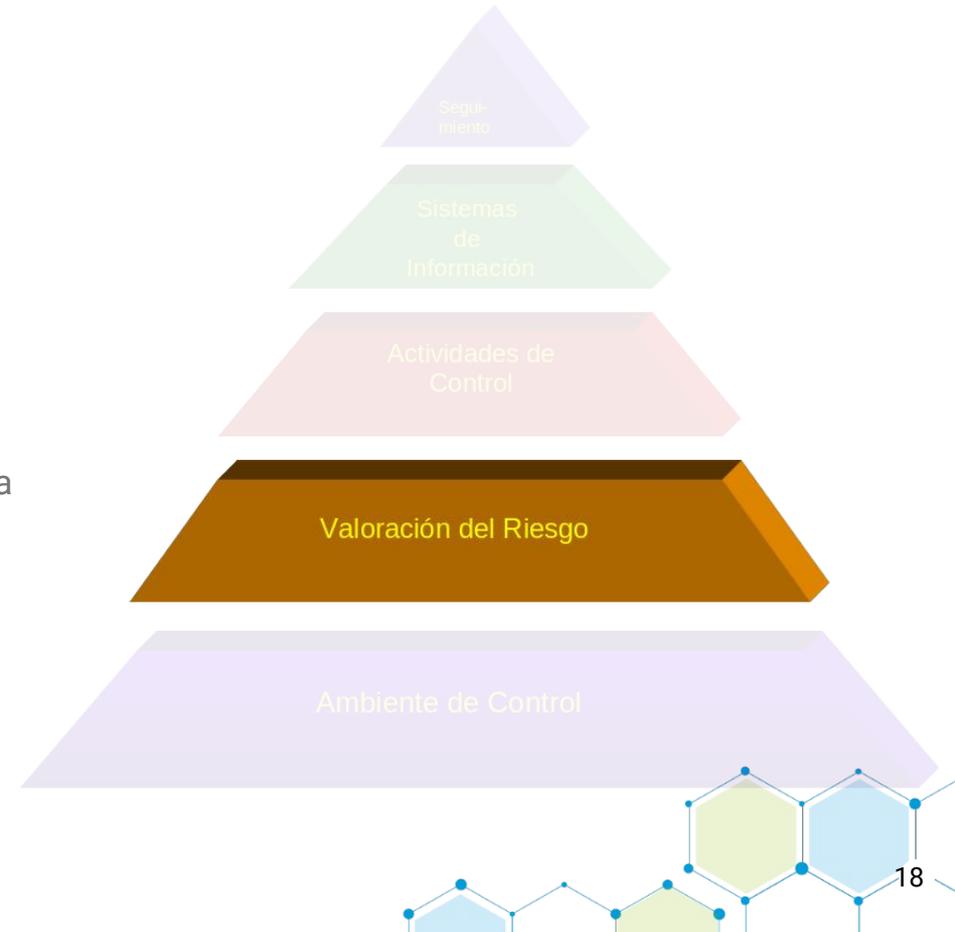
Artículo 18:
Sistema Específico de Valoración del Riesgo Institucional

Todo ente u órgano deberá contar con un sistema específico de valoración del riesgo institucional **por áreas, sectores, actividades o tareas** que, de conformidad con sus particularidades, permita identificar el nivel de riesgo institucional y adoptar los métodos de uso continuo y sistemático, a fin de analizar y administrar el nivel de dicho riesgo.



Componentes funcionales del Sistema de Control Interno

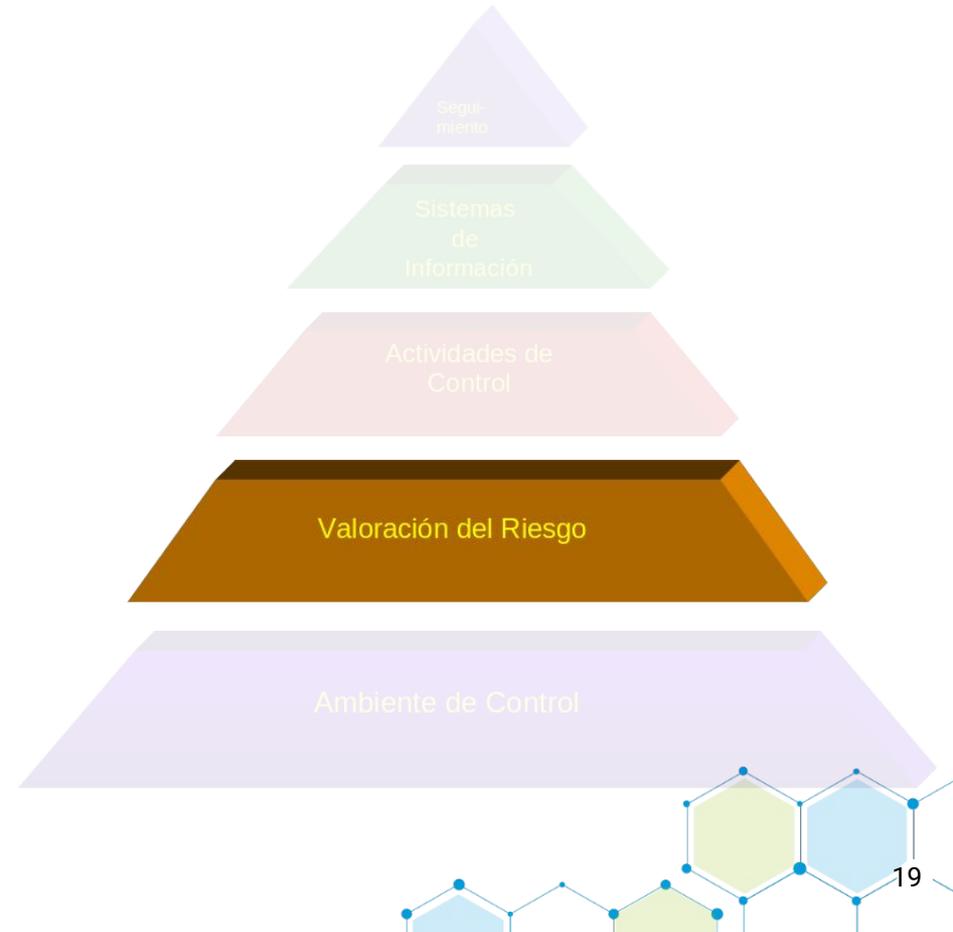
La identificación y análisis de los riesgos que enfrenta la institución, tanto de fuentes internas como externas relevantes para la consecución de los objetivos.



Componentes funcionales del Sistema de Control Interno

Etapas del proceso de Valoración del Riesgo:

- Identificación,
- Análisis,
- Evaluación,
- Administración,
- Revisión,
- Documentación y
- Comunicación de los riesgos institucionales.



Marco de gobierno y gestión de TI

Proceso de Gestión del Riesgo Institucional

Plan Estratégico Institucional 2021-2025
Planes Tácticos de las Unidades
Planes Anuales Operativos de las Unidades
Riesgos en TI

Herramienta informatizada



Marco de gobierno y gestión de TI



UNIVERSIDAD DE
COSTA RICA

Rectoría

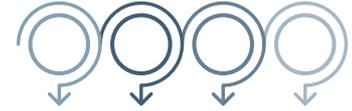
Gestión institucional del riesgo y **Aplicación en TI**

Impulso a la estrategia de protección de activos y atención de riesgos. Sensibilizando al ciudadano digital universitario de las mejores prácticas de manejo, escenarios de ataques y una gestión de seguridad integral.





Comunicación digital



Protección

- Cuidados
- Seguridad TI

Exposición:

- Riesgos
- Aspectos remediales

Uso:

- Ciudadanía digital
- Formación y concientización

Acceso:

- Internet & Intranets
- Redes sociales
- Teletrabajo

Fuente: <https://jiece123.wordpress.com/2013/04/18/337/>

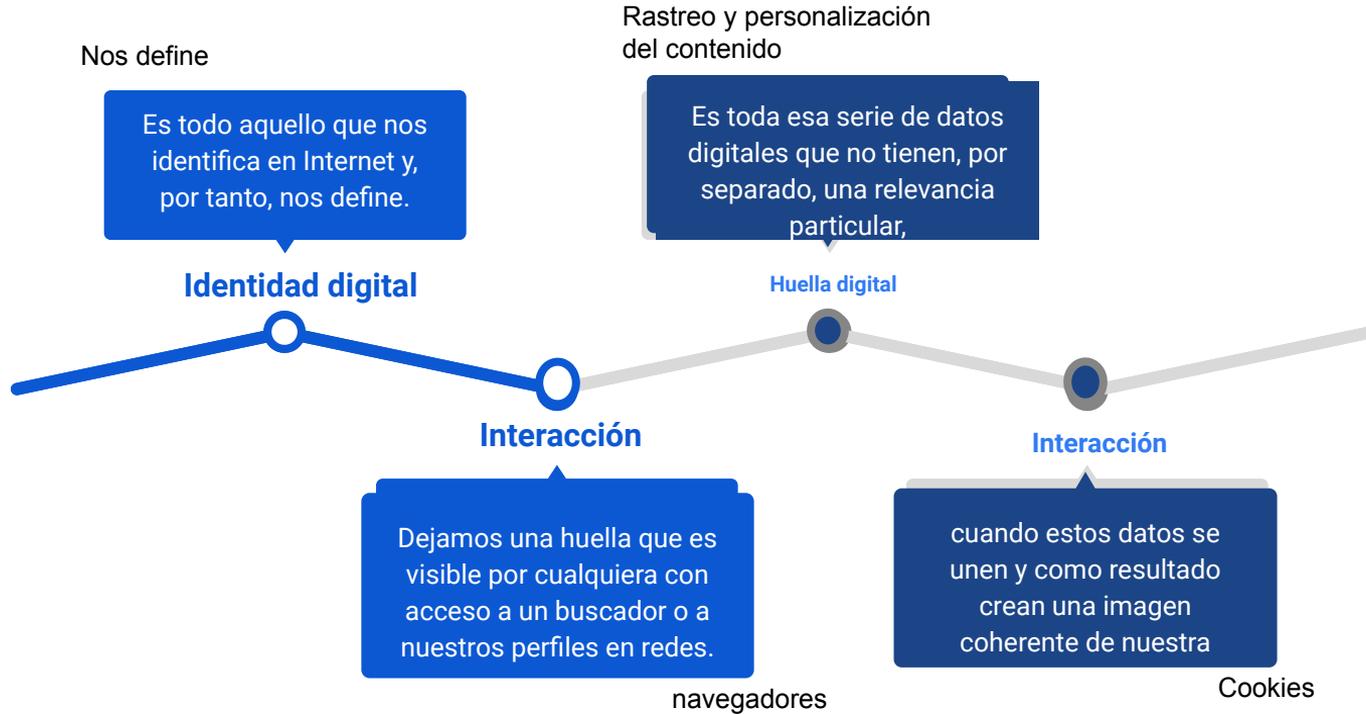
Ciudadanía digital

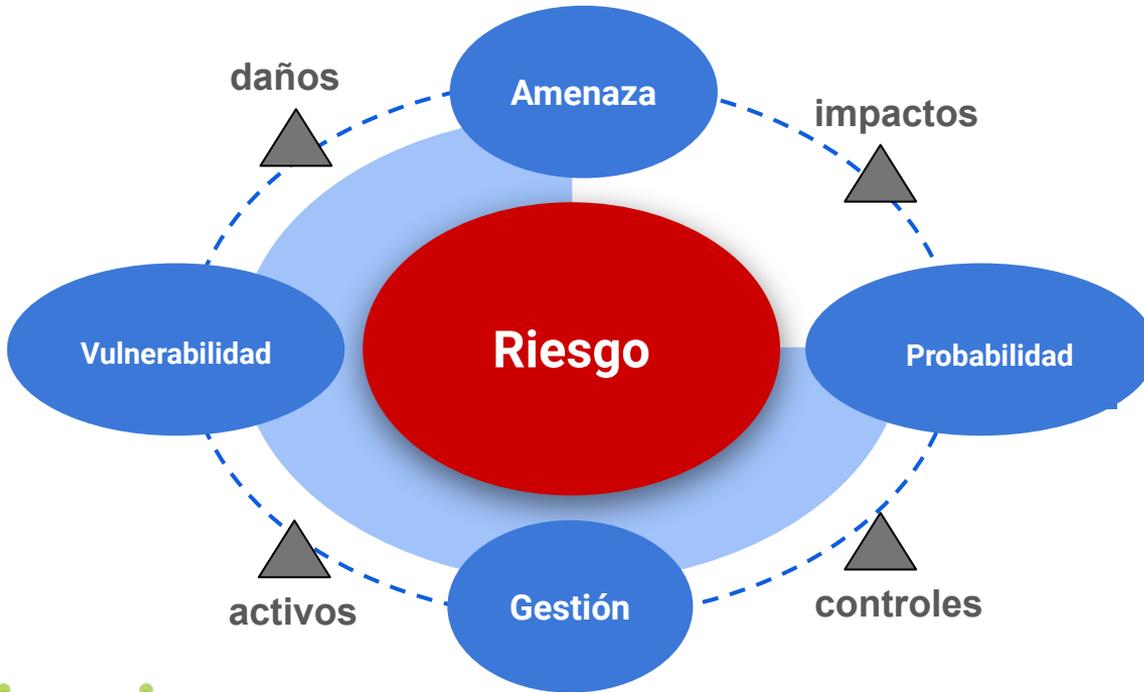
Conjunto de aquellas normas de comportamiento que conciernen al uso de la tecnología



**ÁREAS
RELACIONADAS**

Fuente: Seguridad en línea y Ciudadanía en la era digital, 2022 (<http://ceabad.com>)





El **riesgo** es la probabilidad de que una o varias amenazas se conviertan en un impacto negativo para la organización.

-La vulnerabilidad o las amenazas, por separado, pueden no representar un peligro.

-Pero si se juntan, se convierten en un riesgo, o sea, en la probabilidad de que ocurra un desastre.

Riesgos Información

- Dispersión, pérdida de tiempo.
- Acceso de los niños a información inapropiada y nociva para su edad.
- Acceso a información peligrosa, inmoral, ilícita (pornografía infantil, violencia, racismo, terrorismo,...)



Riesgos Comunicación

- Bloqueo del buzón de correo.
- Recepción de "mensajes basura".
- Recepción de mensajes ofensivos.
- Pérdida de intimidad.
- Acciones ilegales: difundir datos de terceras personas, plagiar, amenazar,...
- Malas compañías.



Riesgos Actividades

- Estafas.
- Compras inducidas por publicidad abusiva.
- Compras por menores sin autorización paterna.
- Robos.
- Actuaciones delictivas por violación de la propiedad intelectual.
- Realización de negocios ilegales.
- Gastos telefónicos desorbitados.



Riesgos Adicciones

- Adicción a buscar información.
- Adicción a frecuentar las Redes Sociales.
- Juego compulsivo.
- Compras compulsivas.

Fuente: <https://www3.gobiernodecanarias.org/medusa/ecoescuela/seguridad/riesgos-asociados-al-uso-de-las-tecnologias/riesgos/>



Algunos riesgos en el uso TIC



Fuente: Seguridad en línea y Ciudadanía en la era digital, 2022 (<http://ceabad.com>)

Ataque de Phishing



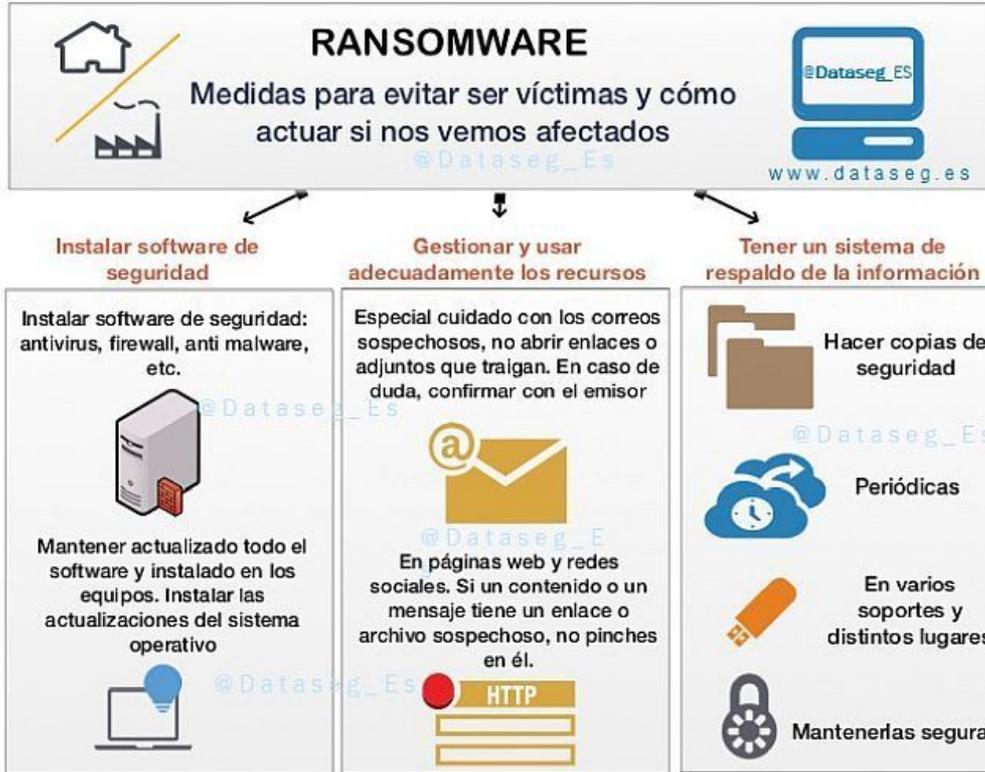
Fuente: <https://www.esferize.com/que-es-el-phishing-como-funciona-y-como-protegerse/>



Fuente: <https://es.safetymdetectives.com/blog/que-es-la-ingenieria-social-y-por-que-es-una-amenaza/>



Ataque de Ransomware



@Dataseg_Es



Y, SI TE VES AFECTADO



@Dataseg_Es



Fuente: <https://dataseg.es/proteccion-de-datos/ransomware-recomendaciones-seguridad/>



Protege tu privacidad

¿Contarías lo que has hecho el fin de semana a una persona desconocida en la cola del cine?
¿Mostrarías las fotos de tus amigos/as durante la fiesta del fin de semana a una persona en el autobús? ¿Entonces por qué lo haces en internet?

Tus redes sociales deben ser **PRIVADAS**.

Cuida tu huella digital



Todo lo que haces, dices y subes a Internet deja un rastro y forma tu "huella digital".

La huella digital es rastreable y puedes dejar información que te puede hacer daño en un futuro si no cuidas lo que publicas.

Piensa antes de publicar



Antes de hacer un comentario o subir una fotografía hazte una pregunta ¿es realmente necesario que publique esta en Internet? ¿me va a traer algún tipo de beneficio? ¿Qué cosas pueden pasar si lo hago? ¿Puede dañarme a mí o a otras personas?



No dar datos personales

No des información sobre dónde vives, estudias o por dónde sales.

Nadie necesita saber tu nombre y apellidos, número de teléfono o cualquier dato de tipo personal.

Ten en cuenta que todo lo que publiques en Internet puede utilizarse para hacerte daño.

Cuidado con los desconocidos/as



En internet hay muchas personas que se dedican a crearse perfiles falsos para conseguir información y otras cosas de menores en la red.

No te fíes de cualquier persona con la que hables en tus redes sociales y no conozcas



Contraseñas seguras

Pracura no usar las mismas contraseñas en todas tus cuentas.

Cambia tus contraseñas cada cierto tiempo y que sean seguras. Para ello usa mayúsculas, minúsculas, números y símbolos.

No participes de mensajes hirientes



Hacer daño en Internet es muy sencillo porque no vemos la reacción que provocamos en las víctimas.

No participes en grupos para reírse de otras personas, compartas imágenes que pueden dañar o escribas mensajes que pueden provocar una reacción grave.

Cuida tu comportamiento online



Insultar, faltar al respeto, reírse de otras personas y tener comportamientos negativos online es muy sencilla.

Ten en cuenta que lo que haces en internet está directamente ligado a tu vida real y puede traerte consecuencias negativas, como denuncias.



Fuente: <https://www.asociacionrea.org/pautas-de-seguridad-en-internet/>



Protección datos en teletrabajo

Asegúrate que el **sistema operativo** de tu dispositivo está **actualizado**.

Debes disponer de un **antivirus actualizado** en tus dispositivos.



Comprueba los **programas** instalados y que estén **actualizados**.



Protege la red WiFi de tu casa.

Cambia el nombre y contraseña de tu red WiFi y la contraseña de la página de configuración del router.



Crea contraseñas complejas y exclusivas para prevenir la filtración de datos.



Realiza **conexiones seguras** siempre a través de la **VPN**.



No uses redes wifi públicas para teletrabajar.



Respetar el deber de secreto profesional. Evita el acceso a información corporativa por familiares.

Bloquea la pantalla del dispositivo si te ausentas o **apágalo** si vas a dejar de usarlo.



No copies información corporativa a los servicios en la nube (Google Drive, Dropbox...)



Cuidado con la copia de información corporativa al equipo personal.



Revisa las pantallas y contenidos que compartes en sesiones de videoconferencia.



Comprueba donde imprimes documentación sensible, no estés en la oficina.



Recuerda aplicar las buenas prácticas...

- Correo electrónico
- Phishing
- Malware



Fuente: <https://sum.jccm.es/node/38>

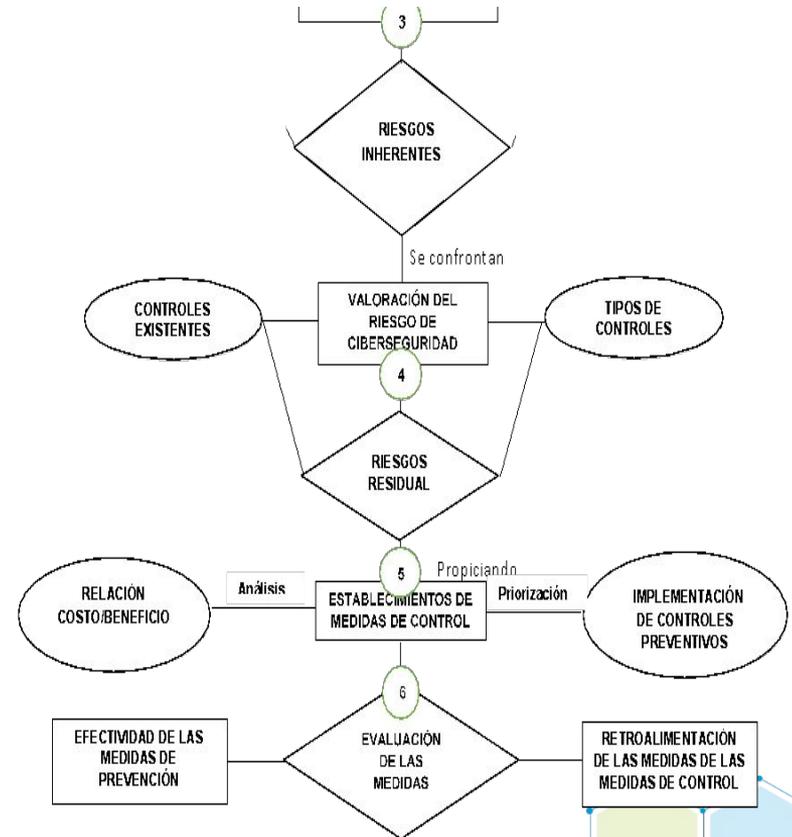
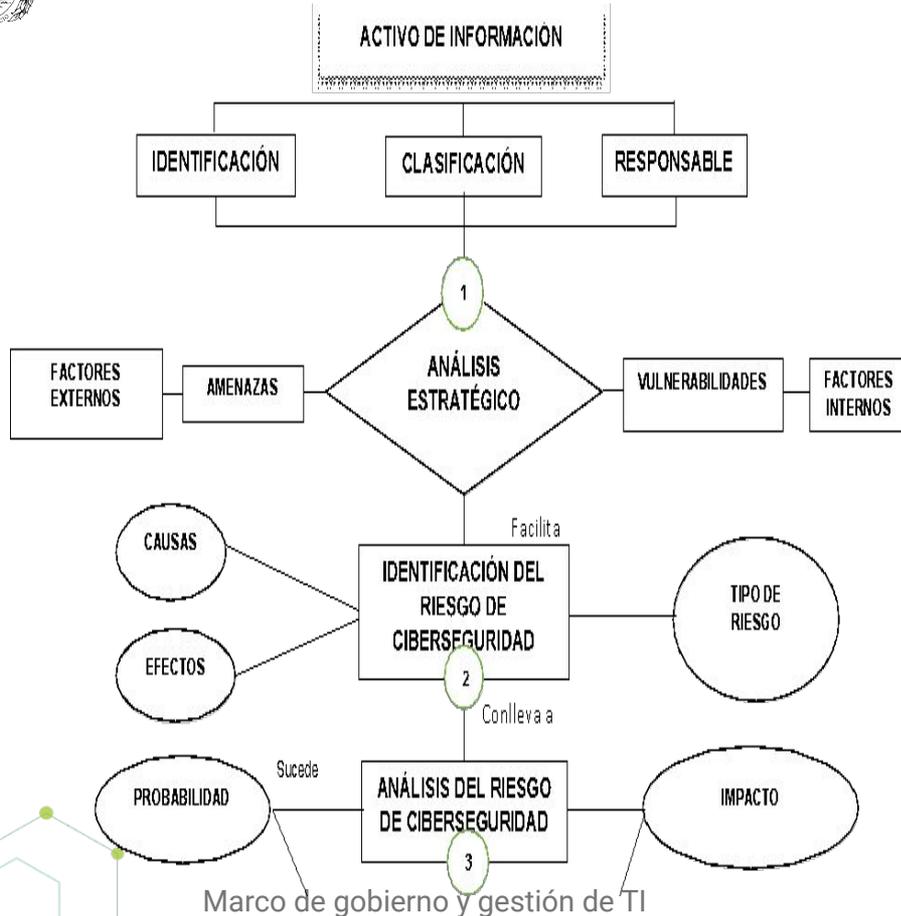
Marco de gobierno y gestión de TI

- 1** Gestionar las cookies
Bloquear cookies en navegadores
- 2** Mejorar la comprensión de los problemas
La privacidad, configuraciones por defecto
- 3** Herramientas para mejorar la privacidad
¿Qué buscan los proveedores?
- 4** Revisar configuración privacidad
Tomar el control de la información que deseamos compartir
- 5** Verificar qué permisos se aplican a las fotografías que sube
Aunque un sitio prometa privacidad, podría haber una violación involuntaria





Metodología Gestión de riesgos TI



Fuente: <https://www.redalyc.org/journal/5713/571361695004/html/>

Pasos metodológicos: Contexto, evaluación y control del riesgo



Consecuencia			Frecuencia					
Personas	Activos	Ambiente	Remoto	Improbable	Poco Probable	Probable	Muy Probable	Frecuente
Crítico			Yellow	Orange	Red	Red	Red	Red
Mayor			Yellow	Yellow	Orange	Red	Red	Red
Serio			Green	Yellow	Orange	Red	Red	Red
Moderado			Green	Green	Green	Yellow	Yellow	Orange
Menor			Green	Green	Green	Yellow	Yellow	Orange
Insignificante			Green	Green	Green	Green	Yellow	Yellow

■ Riesgo Bajo
 ■ Riesgo medio
 ■ Riesgo Medio Alto
 ■ Riesgo Alto

Arrows in the matrix indicate risk transitions:

- White circle (Inherent) to Grey circle (Real) to Black circle (Projected)
- Black circle (Projected) to Yellow (Medium) cell
- Grey circle (Real) to Yellow (Medium) cell
- White circle (Inherent) to Yellow (Medium) cell



CATEGORÍA DE PRODUCTO	ÁMBITO DE APLICACIÓN				
	Gestión de acceso e identidad	Seguridad en el puesto de trabajo	Seguridad en aplicaciones y datos	Seguridad en los sistemas	Seguridad en la red
Anti-fraude Anti-phishing, Anti-spam, Herramientas de filtrado de navegación, UTM, Appliance		✓	✓	✓	✓
Anti-malware Anti-virus, Anti-Adware, Anti-spyware, UTM, Appliance		✓	✓	✓	✓
Auditoría técnica Análisis de logs y puertos, vulnerabilidades, Auditoría de contraseñas, Auditoría de sistemas y ficheros	✓		✓		✓
Certificación normativa SGSI, Análisis de riesgos, Planes y políticas de seguridad, Normativas de seguridad		✓	✓	✓	✓
Contingencia y continuidad H. de gestión de planes de contingencia y continuidad, Copias de seguridad, Infraestructura de respaldo, Virtualización, Cloud		✓	✓	✓	✓
Control de acceso y autenticación Control de acceso a red, NAC, Gestión de identidad y autenticación, Single Sign-On, Certificados digitales, Firma electrónica	✓				

Marco de gobierno y gestión de TI

Fuente: INCIBE

CATEGORÍA DE SERVICIO	ÁMBITO DE APLICACIÓN			
	Personas	Información	Infraestructuras	Negocio
Auditoría técnica test de intrusión, <i>hacking</i> ético, análisis de vulnerabilidades, ingeniería de seguridad, auditorías de código, auditoría forense		✓	✓	
Certificación de normativa SGSI, certificación y acreditación, planes y políticas de seguridad, análisis de riesgos	✓	✓	✓	✓
Contingencia y continuidad copias de seguridad remotas (backup), planes de contingencia, centros de respaldo				✓
Cumplimiento legal consultoría legal, auditoría de legislación, borrado seguro, destrucción documental	✓	✓	✓	
Formación y concienciación formación en materia de ciberseguridad, certificación profesional, sensibilización y concienciación	✓			
Gestión de incidentes prevención, detección, respuesta a incidentes de seguridad	✓	✓	✓	
Implantación de soluciones soluciones de ciberseguridad, ciber-resiliencia, ciberseguridad industrial			✓	
Seguridad en la nube <i>software</i> como servicio (SaaS), plataforma como servicio (PaaS), infraestructura como servicio (IaaS)		✓	✓	✓

Estrategia de Seguridad TI

Busca evitar el acceso no autorizado a activos de la organización, como computadoras, redes, servicios y datos.

Servicios
Personas, Información,
infraestructura y negocio



Productos

- Gestión de acceso e identidad
- Protección en el puesto de trabajo
- Seguridad en aplicaciones y datos
- Seguridad en los sistemas
- Seguridad en las redes

Perímetro | Aplicaciones | Datos

* **La seguridad total no existe** y menos cuando estamos los humanos de por medio.

Marco de gobierno y gestión de TI



UNIVERSIDAD DE
COSTA RICA

Rectoría

Gestión institucional del riesgo y Aplicación en TI

César Picado

Oficina de Planificación, UCR

Abel Brenes Arce

Centro de Informática, UCR

17 agosto 2022

Marco de gobierno y gestión de TI

