TEC | Tecnológico de Costa Rica

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

DATIC
DEPARTAMENTO DE ADMINISTRACION DE TECNOLOGIAS DE INFORMACION Y COMUNICACIONES

CONTROL DE CAMBIOS

Elaborado por: MPD. Luis Felipe Picado Valverde, Gestión de TI, DATIC.	**Última revisión por:** Natalia Morales Madriz, Coordinadora de Sistemas de Información, DATIC. Alfredo Villareal Rodríguez, Coordinador de Infraestructura Tecnológica, DATIC. Gustavo Bolaños Solano, Coordinador de Soporte Técnico, DATIC.
Versión No.1 **Revisar y actualizar:** Anualmente	**Aprobado por:** MGP. Andrea Cavero Quesada, Directora DATIC. TEC | Tecnológico de Costa Rica Firmado digitalmente por ANDREA MARCELA CAVERO QUESADA (FIRMA) Fecha: 2023.04.28 11:22:31 -06'00'

ALCANCE

Los siguientes lineamientos aplican para el personal del Instituto Tecnológico de Costa Rica, busca establecer diferentes normas que regulen la seguridad de activos de información, seguridad lógica, física, del personal y de operaciones de TI.

DESCRIPCIÓN DE LOS LINEAMIENTOS

Los siguientes lineamientos poseen todas las acciones tendientes a la detección y corrección de riesgos presentes en el Instituto Tecnológico de Costa Rica. Se busca su definición porque permite establecer un rumbo en cuanto a la seguridad del manejo de las tecnologías de información.

Además, atienden a lo dispuesto en el Marco de Gobierno y Gestión de TI del Instituto Tecnológico de Costa Rica. Específicamente al Objetivo de Gestión de Seguridad de la Información.

LINEAMIENTOS DE CLASIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN

TEC | Tecnológico de Costa Rica

Se refiere a las tareas relacionadas con el manejo de activos de información, las cuales se basan en las propiedades de integridad, disponibilidad y confidencialidad, asimismo, se evalúa el impacto que tendría el irrespeto a alguna propiedad.

Definición de responsabilidades

Se debe definir el **Equipo de Seguridad** dentro del Instituto Tecnológico de Costa Rica. Este se encargará de establecer las políticas de seguridad de la información y de velar por el cumplimiento de estas. Es necesario incorporar el rol que desempeña la persona, nombre, área o departamento al que pertenece, cuáles serán sus funciones y responsabilidades en el equipo.

Dicho equipo será designado por el Comité Estratégico de TI (CETI) y será a este órgano a quién le rendirá cuentas.

Dentro de las funciones de este equipo se encuentran:

- Revisar los lineamientos o disposiciones en materia de seguridad de la información y las responsabilidades generales en materia de seguridad de la información.
- Monitorear cambios significativos en la exposición de activos de información frente a las amenazas
- Revisar y monitorear los incidentes relativos a la seguridad.
- Revisar y aprobar las principales iniciativas para incrementar la seguridad de la información
- Acordar funciones y responsabilidades específicas relativas a seguridad de la información
- Acordar metodologías y procesos específicos relativos a la seguridad de la información
- Acordar, brindar apoyo y difusión, a las iniciativas de seguridad de la información
- Evaluar y coordinar la pertinencia y la implementación de controles específico de seguridad de la información para nuevos sistemas o servicios.
- Establecer los responsables de comunicar la creación y modificaciones de las políticas. Además, definir a cuáles colaboradores se deberán informar los cambios y los medios de comunicación que se utilizarán para difundirlas.
- Sugerir al CETI o al DATIC la implementación de medidas, creación de procedimientos o asignación de responsabilidades, según corresponda, para velar por la seguridad de la información

TEC | Tecnológico de Costa Rica

LINEAMIENTOS DE SEGURIDAD LÓGICA

Los lineamientos de seguridad lógica se refieren a las medidas internas que se toman a nivel institucional para el manejo de los aspectos relacionados a los controles de acceso, manejo de contraseñas, ataques a la red, protección y prevención de amenazas a los sistemas.

Control de acceso

• Establecer mecanismos de control de acceso a los sistemas de información institucionales de manera que se garantice que, únicamente los usuarios autorizados tengan acceso al sistema velando así por la integridad de la información.

• Controlar el acceso a la información, a los servicios, sistemas y procesos institucionales con base en las directrices, estándares y procedimientos previamente aprobados por la comisión de seguridad y/o la dirección del DATIC.

• Asignar la administración de los permisos de acceso a los sistemas institucionales al Departamento de Administración de Tecnologías de Información y Comunicaciones (DATIC).

• Establecer procedimientos formales para la definición de los niveles de acceso y para la asignación de permisos a los sistemas institucionales.

• Establecer procedimientos formales para la administración y revisión periódica de permisos de acceso, registro y eliminación de usuarios.

• Toda acción referente al manejo y gestión de las cuentas de usuario del dominio @itcr.ac.cr (@tec.ac.cr) o @estudiantec.cr, debe solicitarse según las vías que establezca el DATIC en sus procedimientos.

• Mientras se considere técnicamente viable y necesario, todo equipo computacional o dispositivo tecnológico del ITCR debe pertenecer al dominio institucional.

• Las jefaturas deben tramitar la apertura, modificación o cierre de cualquier cuenta de usuario, utilizando los procedimientos establecidos por el DATIC y por el departamento de Gestión de Talento Humano.

Manejo de contraseñas

• Asignar al usuario la responsabilidad por el manejo de la contraseña de la o las cuentas institucionales asignadas, definiendo de manera clara las consecuencias relacionadas con el mal uso, descuido o negligencia

• El DATIC debe definir los requisitos mínimos que debe cumplir en cuanto al formato de las contraseñas y establecer un mecanismo de protección para mantener esta información confidencial.

• Cumplir con los criterios establecidos de longitud, tipo de caracteres, mayúsculas y minúsculas, entre otros, según corresponda, para las contraseñas del dominio @itcr.ac.cr (@tec.ac.cr) y @estudiantec.cr.

• Cumplir con los criterios establecidos de longitud, tipo de caracteres, mayúsculas y minúsculas, entre otros, según corresponda, para las contraseñas de aplicaciones y bases de datos.

• Establecer procedimientos de recuperación de contraseñas en las cuentas institucionales (de funcionarios y estudiantes).

• Establecer períodos de validez para las contraseñas de cuentas institucionales.

• Establecer períodos de validez para las contraseñas de aplicaciones y bases de datos, cuando se expira ese período la contraseña deberá ser actualizada

• Aplicar acciones de bloqueo de las cuentas institucionales en caso de detectar actividades sospechosas con el fin de prevenir cualquier tipo de violación a la seguridad o robo de identidad.

• Establecer los mecanismos y procedimientos necesarios para que ante actividades sospechosas el usuario pueda volver a recuperar su cuenta.

• Aplicar mecanismos de inicio de sesión y monitoreos para permitir el registro y la detección de acciones que puedan afectar la seguridad de la información. Será responsabilidad del DATIC definir el tiempo de conservación de estos datos.

• Almacenar y resguardar las contraseñas en los servidores institucionales, aplicando mecanismos de encriptación para garantizar que esta información no sea visible.

• Establecer los mecanismos de control, procedimientos y los requisitos necesarios para que los usuarios utilicen privilegios elevados en los equipos institucionales.

Protección de software malicioso

• Establecer procedimientos para la gestión de software institucional, monitoreo, detección y control de software malicioso en los equipos computacionales.

• Denegar la instalación de software en los equipos de computación institucional, ya que solamente será permitido instalar el software autorizado por el Departamento de Administración de Tecnologías de Información y Comunicaciones (DATIC).

• Establecer mecanismos de revisión periódica a los equipos institucionales con objetivo de controlar el software instalado en los mismos. En caso de identificarse una anomalía o software malicioso, se realizarán las acciones necesarias para eliminar el software malicioso o no autorizado.

• Regular el uso de equipos institucionales de los usuarios. Esta información será comunicada por los medios oficiales, donde sea visible, para asegurar que los usuarios tengan conocimiento y hagan uso correcto del equipo.

Ataques a la red

- Establecer procedimientos para la identificación y gestión de la seguridad mínima que se debe tener ante un ataque de red.

- Implementar mecanismos de filtrado de red, como firewalls y software de detección de intrusos.

- Implementar las políticas adecuadas para controlar el tráfico de red entrante y saliente.

- Establecer controles especiales para salvaguardar la confidencialidad e integridad de los datos que pasan a través de redes públicas o inalámbricas para proteger los sistemas y aplicaciones conectados

- Llevar a cabo pruebas de penetración periódicas para determinar la idoneidad de la protección de la red mediante las herramientas de fábrica del proveedor del equipo.

- Establecer los controles necesarios para mantener la disponibilidad de los servicios de red y las computadoras conectadas.

- Definir mecanismos de autenticación para los sistemas en la red institucional del ITCR.

- Aplicar tecnologías para la seguridad de los servicios de red, como autenticación, cifrado y controles de conexión de red sean tanto de manera interna o externa.

- Establecer procedimientos para el uso del servicio de red para restringir el acceso a servicios o aplicaciones dentro de la red institucional.

- Definir los roles y niveles de acceso a los sistemas para el manejo de la información por parte de los equipos de administración de red.

- Establecer mecanismos de control en los equipos de red para garantizar la seguridad ante la comprobación de la autenticidad de sitios web.

- Actualizar el software en los equipos de administración de la red para garantizar una mayor protección ante ataques a estos equipos.

- Actualizar el software en los equipos de usuario final para garantizar una mayor protección ante ataques.

Ataques a sistemas de información

- Establecer procedimientos para la definición y gestión de la seguridad mínima que deben tener los sistemas de información ante un ataque de seguridad.

- Definir e implementar mecanismos de protección de código fuente y datos de los sistemas de información.

- Establecer mecanismos de defensa que permitan prevenir y evitar ataques a los datos de los sistemas de información.

- Realizar revisiones periódicas a los sistemas de información para identificar las vulnerabilidades existentes y tomar acciones correctivas.

- Definir controles en los sistemas de información para prevenir las pérdidas, modificaciones y/o el uso no autorizado de los datos. Dichos controles incluyen validación de datos de entrada, verificación de datos generados y validación de datos de salida.

- Definir requisitos mínimos de cumplimiento en el desarrollo, arquitectura e implementación de estándares de seguridad para todos los sistemas institucionales, ya sea desarrollados en la institución o adquiridos a terceros para velar por la protección de la información.

- Implementar técnicas y mecanismos criptográficos estandarizados en los sistemas de información para velar por la protección de la confidencialidad, autenticidad e integridad de la información sensible.

- Concientizar a los funcionarios de la responsabilidad exclusiva de los mecanismos de acceso que les sean otorgados por parte del DATIC, ya que son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ninguna persona externa.

- Verificar y tomar medidas inmediatas ante reportes de posibles vulnerabilidades encontradas por los usuarios en los sistemas de información

- Velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que dicho sistema trate.

- Llevar una bitácora de acceso a los sistemas y sus funcionalidades con el objetivo de identificar posibles amenazas.

LINEAMIENTOS DE SEGURIDAD FÍSICA

Estos lineamientos se relacionan con el manejo de los activos físicos los cuales se pueden ver amenazados si no se siguen las medidas preventivas necesarias. Se involucran principalmente las medidas de regulación de acceso a los dispositivos físicos del Instituto Tecnológico de Costa Rica.

Será el DATIC la instancia que deberá velar por el cumplimiento de estos lineamientos.

• Mantener actualizada la siguiente información de los equipos:

- Nombre del equipo computacional.
- Descripción de la información que almacena.
- Localización.
- Controles de acceso que implementa.
- Mecanismos de protección ante amenazas físicas y ambientales.
- Mecanismos de monitoreo y control.

• Registrar y monitorizar todos los puntos de entrada a las instalaciones de TI. Es necesario registrar a todos los visitantes de los sitios que almacenen información o equipos sensibles, incluidos contratistas, proveedores y personas externas al DATIC.

• Monitorear la estadía de los visitantes al centro de datos por medio de un acompañamiento de un miembro responsable durante su estancia en las instalaciones del DATIC.

• Restringir y monitorizar el acceso al centro de datos, mediante el establecimiento de restricciones de perímetro, como vallas, paredes y dispositivos de seguridad en puertas interiores y exteriores.

• Garantizar que los perfiles de acceso permanezcan actualizados. Basar el acceso a las instalaciones de TI (sala de servidores, edificios, áreas o zonas) en el cargo y las responsabilidades.

• Implementar acciones de seguridad contra incendios, como alarmas que alerten sobre un riesgo latente, estos mecanismos deben ser monitoreados y probados para velar por la seguridad de las instalaciones.

• Establecer mecanismos de control de acceso en las entradas a sitios que resguarden información y equipo sensible, para que únicamente puedan ingresar quienes están autorizados para dichos fines.

• Monitorear por medio de cámaras de seguridad el acceso a sitios que resguarden información y equipo sensible, asimismo, alertar en caso de descubrir un acceso no autorizado.

TEC | Tecnológico de Costa Rica

LINEAMIENTOS DEL USO DE ACTIVOS DE INFORMACIÓN

Se basa en un conjunto de normas que regulan la utilización de los equipos de cómputo, el internet dentro de la institución y el correo institucional con el objetivo de disminuir fallas en la seguridad del DATIC.

Uso del equipo de cómputo

• Realizar el mantenimiento correctivo y preventivo de los recursos tecnológicos de la institución por parte del DATIC.

• Acatar los procedimientos que defina el DATIC para diagnosticar problemas en los equipos de cómputo e implementar las recomendaciones brindadas.

• Utilizar los equipos de cómputo asignados a los diferentes Departamentos, dependencias y usuarios de la institución únicamente para cumplir con los fines y objetivos del ITCR. Al ser bienes públicos que forman parte del patrimonio institucional, los mismos no pueden ser utilizados para realizar actividades personales o con fines lucrativos.

• Considerar toda la información que esté almacenada en los equipos de cómputo y dispositivos de almacenamiento de la institución de carácter laboral y, por ende, propiedad del ITCR.

• Restringir la instalación de hardware o software no autorizado previamente por el DATIC.

• Restringir la modificación y reparación de los equipos de cómputo y sus componentes sin la autorización del DATIC.

• Restringir la modificación de la configuración base de hardware definida por el DATIC, así como la configuración de software general del equipo de cómputo.

Uso del equipo de cómputo

• Establecer políticas que regulen el uso del Internet provisto por la Institución junto con prohibiciones y sanciones.

Uso del equipo de cómputo

• Identificar los riesgos asociados al uso inadecuado del correo institucional y aplicar las medidas de mitigación que correspondan para atender la eventual materialización de dichos riesgos.

• Cumplir con lo establecido en el Reglamento de Correo Electrónico Institucional.

LINEAMIENTOS DE SEGURIDAD PERSONAL

Conjunto de normas relacionadas a la seguridad de la información que deberán ser aplicadas en la gestión del recurso humano de la institución.

- Clasificar los datos recolectados por el Instituto Tecnológico de Costa Rica en categorías que delimiten su tratamiento.

- Determinar el nivel de confidencialidad de las categorías de datos para garantizar que se brinde el tratamiento adecuado.

- Establecer las responsabilidades y obligaciones en cuanto al uso de los activos de información institucionales, dirigidas al personal que los utilice.

- Definir términos, condiciones y acuerdos de confidencialidad para el manejo de la relación entre la institución y el personal.

- Establecer y hacer uso de mecanismos para mitigar el riesgo de robo, fraude y mal uso de los recursos de información.

- Aplicar lo dispuesto en la regulación nacional con respecto a la protección de la persona frente al tratamiento de sus datos personales.

LINEAMIENTOS DE SEGURIDAD DE LAS OPERACIONES

Se basa en un conjunto de normas que rigen en la definición y gestión de operaciones que involucren activos de información, tienen como objetivo minimizar el riesgo de fallas y la continuidad de las operaciones de la institución. Además, busca asegurar el funcionamiento correcto y seguro de las instalaciones de procesamiento de información.

- Ejecutar procedimientos operativos con el objetivo de mantener y ejecutar tareas operativas de manera confiable y consistente.

- Gestionar la operación de los servicios tercerizados de TI para mantener la protección de la información institucional y la confiabilidad de la provisión del servicio.

- Monitorizar la infraestructura de TI y eventos relacionados mediante el almacenamiento de información cronológica en los logs de operación que permita la reconstrucción y revisión de las secuencias temporales de las operaciones y otras actividades asociadas o que apoyan las operaciones. El tiempo de conservación de esta información deberá ser definida por DATIC.

- Implementar medidas de protección contra factores medioambientales del centro de datos, por ejemplo: controles de temperatura, de humedad, entre otros.

- En cuanto a respaldos de informacion, el DATIC es el responsable de definir la información de las bases de datos institucionales que se respalda, cada cuánto tiempo se respalda, por cuánto tiempo se mantienen los respaldos, asi como también definir un plan de pruebas y recuperacion de informacion.

- Gestionar las instalaciones, incluidos los equipos de suministro eléctrico y comunicaciones, alineados con las leyes, reglamentos existentes, requisitos técnicos y de la institución, especificaciones del proveedor, y las directrices de salud y seguridad.

- Desarrollar procedimientos de seguridad de TI que incluyan un esquema de documentación de informes sobre incidentes de seguridad que se hayan presentado anteriormente en el DATIC

LINEAMIENTOS DE CONCIENTIZACIÓN Y CAPACITACIÓN

Estos lineamientos aplican de manera transversal al resto de medidas que se adopten para la seguridad de la información del ITCR y deberán ser: promovidos por el equipo de seguridad de la información y apoyados por el DATIC, el CETI y en caso de ser necesario con el Departamento de Gestión del Talento Humano.

- Desarrollar dentro de la organización actividades de concientización y capacitación en temas de seguridad de la información dirigidos a toda la población institucional.

- Concientizar a la población institucional mediante correos informativos, sobre el manejo y la destrucción del papel de desecho que contenga información institucional, eliminación de contraseñas visibles en escritorios, superficies de computadoras o cualquier otro lugar visible por terceros.

- Definir una documentación de medidas de seguridad, reglas y regulaciones que sirva como referencia para la consulta sobre aspectos de seguridad de TI.

LINEAMIENTOS DE PROTECCIÓN DE DATOS PERSONALES

Estos lineamientos aplican de manera transversal a todas las actividades que realice la Institución que implican la utilización de datos personales con la finalidad de velar por el respeto de los derechos y libertades de las personales usuarias con respecto al uso de sus datos personales y su privacidad. Además, del cumplimiento del Reglamento para la aplicación de la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales (ley 8968) del TEC, y la ley 8968 así como su respectivo reglamento.

Al ser los datos personales parte de la información que se está contemplando proteger dentro de los distintos apartados de la presente política. su aplicación misma implica una protección para los datos personales. Sin embargo, cabe resaltar que se recomienda de manera fundamental:

- Cumplir con todo lo estipulado en el Reglamento para la aplicación de la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales (ley 8968) del TEC.
- Realizar una identificación de datos personales utilizados en el TEC por las distintas instancias indicando los tipos de datos personales, los fines para su tratamiento, los medios para tratarlos, así como si se cuenta con el consentimiento respectivo para su tratamiento.
- Establecimiento de las medidas necesarias para que el tratamiento sea legítimo. Refiérase a la Guía para la redacción de consentimientos informados del TEC.
- Analizar los riesgos de los tratamientos de datos personales que se realizan para tomar las salvaguardas que sean necesarias.
- Establecer los periodos de conservación de los datos.
- Para todas las instancias, acatar la Guía de Seguridad de la Información para la Protección de Datos Personales del TEC.

Además, el Equipo de Seguridad de la Información del TEC deberá velar por la actualización de la Guía de Seguridad de la Información para la Protección de Datos Personales del TEC, así como de su cumplimiento.

DATIC

DEPARTAMENTO DE ADMINISTRACION
DE TECNOLOGIAS DE INFORMACION
Y COMUNICACIONES