POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

UNIVERSIDAD EIA

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La política de seguridad de la información de la Universidad EIA permite establecer reglas, directrices y procedimientos establecidos por la institución, para proteger los datos y los sistemas tecnológicos de la información, contra amenazas y riesgos de seguridad.

Esta política busca promover una cultura de seguridad organizacional y establecer un marco de trabajo que garantice la confidencialidad, integridad y disponibilidad de la información. Además, ayudara a cumplir con los requisitos legales y normativos relacionados con la seguridad de la información.

Para toda organización la información es un recurso fundamental para promover el desarrollo, incrementar el nivel de competitividad, tomar decisiones acertadas y lograr el cumplimiento de los objetivos estratégicos. La universidad EIA genera, recibe, comparte y almacena información en sus procesos cotidianos, a través de sus diferentes programas académicos, investigaciones, estrategias, productos y servicios, además de la información referente a sus empleados y estudiantes.

En este contexto, la información es para la institución uno de los activos más importantes, al igual que las personas, los procesos, la tecnología, espacios físicos, entre otros, los cuales deben protegerse por el valor que tienen para la Universidad por ser necesarios para mantener la operación de los procesos institucionales.

MARCO NORMATIVO

La presente política está alineada con las siguientes disposiciones normativas en aras de trabajar por la seguridad de la información.

- Constitución Política de Colombia.
  "Artículo 15: Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptados o registrados mediante orden judicial, en los casos y con las formalidades que establezca la ley. Con el fin de prevenir la comisión de actos terroristas, una ley estatutaria reglamentará la forma y condiciones en que las autoridades que ella señale, con fundamento en serios motivos, puedan interceptar o registrar la correspondencia y demás formas de comunicación privada, sin previa orden judicial, con aviso inmediato a la Procuraduría General de la Nación y control judicial posterior dentro de las treinta y seis (36) horas siguientes. Al iniciar cada período de sesiones el Gobierno rendirá informe al Congreso sobre el uso que se haya hecho de esta facultad. Los funcionarios que abusen de las medidas a que se refiere este artículo incurrirán en falta gravísima, sin perjuicio de las demás responsabilidades a que hubiere lugar. Para efectos tributarios judiciales y para los casos de inspección, vigilancia e intervención del Estado, podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley.
- Ley estatutaria 1581 de 2012 por la cual se dictan disposiciones generales para la protección de datos personales.
- Decreto 1377 de 2013 por el cual se reglamenta la ley estatutaria 1581 de 2012.
- Código de Buen Gobierno EIA, el cual tiene por objetivo establecer políticas de buenas prácticas para promover una mejor gestión de los recursos y proporcionar un instrumento ágil en el cumplimiento de la misión.
- Estatutos Generales, que jurídicamente definen el quehacer institucional.

- Proyecto Institucional, que refleja la dinámica institucional para responder al compromiso que ha asumido con el Estado y a la sociedad de formar profesionales de pregrado y posgrado de alta calidad.
- Política de transparencia, acceso a la información y anticorrupción de la Universidad EIA, como marco de referente para la construcción e implementación de acciones orientadas a la protección del derecho a saber, la calidad de la información, la trasparencia y legalidad.
- Política de tratamiento de datos personales Universidad EIA.
-

COMPROMISO

La Universidad EIA declara su compromiso con la seguridad de la información garantizando la confidencialidad, integridad y disponibilidad de la misma.

Artículo 1: Objetivos de la política

La presente política tiene como objeto establecer una serie de estrategias, acciones y directrices encaminadas a lograr la seguridad de la información, entre ellas:

a) Establecer las normas y medidas de control que deben seguir los miembros de la Universidad EIA para el uso de los activos de información.
b) Mantener la confidencialidad, disponibilidad e integridad de la información personal e institucional.
c) Sensibilizar al, estudiantes, profesores, personal administrativo, investigadores y usuarios externos en el cuidado, protección y responsabilidades asociadas al tratamiento de la información.
d) Minimizar la probabilidad de que se presenten incidentes de seguridad y mitigar el impacto que se pueda generar por los riesgos y amenazas asociados a los activos de información.
e) Dar cumplimiento a las disposiciones legales vigentes y los marcos de buenas prácticas de seguridad de la información.

Artículo 2: Ámbito de aplicación

Esta política aplica a quienes tengan acceso o responsabilidad sobre el tratamiento de la información institucional y a quienes hagan uso de los activos de información e infraestructura tecnológica de la Universidad EIA, incluyendo a estudiantes, egresados, profesores, administrativos, visitantes y terceros con los que la universidad establezca relaciones.

Artículo 3: Aspectos generales

Activos de información[1]

Un activo de información es un elemento tangible o intangible que contiene o utiliza información de valor para la institución o que es necesario para mantener la continuidad de sus procesos. Algunos de los activos de información más comunes incluyen:

I. **Datos y bases de datos:** Información almacenada en bases de datos y otros sistemas de almacenamiento, como registros de estudiantes, información financiera, etc.

II. **Software:** programas y aplicaciones que la institución usa para operar y el código fuente asociado.

[1] Consultado en ChatGPT de OpenAI (Activos de Información) (23/01/2024)

III. **Hardware:** Equipos físicos como servidores, computadores, dispositivos de almacenamiento, etc.

IV. **Redes:** Infraestructura de comunicación que permiten la transferencia de datos entre dispositivos.

V. **Documentación:** Manuales, procedimientos, políticas y otros documentos que contienen información crítica sobre la operación y gestión de la institución.

VI. **Personal:** Los empleados y otros colaboradores que tienen acceso a información sensible y desempeñan un papel crucial en la seguridad de la información.

VII. **Propiedad intelectual:** Patentes, marcas registradas, secretos comerciales y otros activos que representan la propiedad intelectual de la institución.

VIII. **Instalaciones físicas:** Los edificios y lugares físicos donde se almacena, procesa o transmite información.

IX. **Servicios:** Servicios críticos para la operación de la organización que involucran la gestión de información, como servicios en la nube, servicios financieros, etc.

X. **Reputación:** La imagen y la reputación de la institución, que pueden verse afectadas por la pérdida o el mal uso de la información.

Artículo 4: Acceso a los recursos y servicios de TI

A continuación, se definen los lineamientos establecidos para acceder a los diferentes recursos y servicios dispuestos por el área de Tecnologías de información y comunicaciones (TIC) desde la perspectiva de la seguridad informática.

- Los permisos de accesos a los recursos informáticos y servicios de la red deben ser solicitados únicamente por el jefe directo de la persona, por medio de la herramienta de mesa de ayuda https://ayudame.eia.edu.co/
- El jefe o director de cada área es responsable de evaluar periódicamente los permisos de cada usuario en los recursos y sistemas informáticos que administre, como también deberá solicitar por la herramienta de mesa de ayuda la asignación y eliminación de los permisos correspondientes para cada usuario en los recursos y sistemas que administre el área de TIC.
- Ninguna persona debe tener acceso con privilegios de administrador en los computadores de la institución, a menos que tenga una justificación para hacerlo aprobada explícitamente por la dirección de TIC.
- Se deben asignar permisos de acuerdo con cada rol y función que desarrolla cada persona, sin otorgar ningún privilegio diferente a los que sean necesarios para llevar a cabo su labor. Las excepciones deberán ser autorizadas por la Dirección de TIC. El usuario es responsable de usar los privilegios asignados de forma adecuada.
- Los usuarios deberán en todo momento realizar un uso responsable de la información y los sistemas accedidos, garantizando un nivel de seguridad adecuado según los lineamientos establecidos en esta política.

Artículo 5: Usuario de red institucional

El área de TIC asignará a cada empleado un usuario de red y contraseña para acceder a los diferentes servicios informáticos. El empleado debe adoptar las siguientes medidas de control:

I. Este usuario es personal e intransferible y cada persona deberá custodiarlo y no divulgarlo, ya que será responsable de las acciones que se realicen en su nombre.
II. Crear contraseñas de al menos 12 caracteres, que contengan una combinación de letras mayúsculas, minúsculas, números y caracteres especiales.
III. Cambiar la contraseña cuando sospeche que alguien más la conoce, la haya robado o esté suplantando su identidad.

Parágrafo: Cuando un empleado, proveedor, contratista o estudiante termine su vínculo laboral con la Universidad, el usuario será deshabilitado y perderá el acceso a los servicios informáticos a los que tenga derecho con este.

Artículo 6: Cuenta de correo institucional

El área de TIC asignará a cada estudiante y empleado, y en algunos casos a contratistas, una cuenta de correo electrónico para acceder a las diferentes herramientas de intercambio de información como Correo, Sharepoint, Onedrive, Teams, entre otras. Cada persona debe adoptar las siguientes medidas de control:

I. Se prohíbe suplantar la identidad de otro usuario, ceder y divulgar a terceros listas de correo electrónico institucional, así como el envío de mensajes de correo en cadena, correos masivos no institucionales, de contenido comercial de esparcimiento, con fines de lucro o para ofrecer servicios
II. No se deberá abrir enlaces o archivos adjuntos de ningún correo electrónico cuyo origen sea desconocido o de dudosa procedencia.

Parágrafo 1: Para los casos en que se requiera crear cuentas genéricas, los jefes o directores de cada área deberán solicitarlas a través de la herramienta de mesa de ayuda con su respectiva justificación e indicando la persona responsable de la cuenta.

Parágrafo 2: Cuando una persona termine su vínculo laboral o académico con la institución perderá el acceso a esta cuenta de correo electrónico y a las diferentes herramientas a las cuales tenía derecho con esta.

Artículo 7: Proveedores

Aquellos proveedores que por contratos de servicios con la Universidad requieran acceder a los activos de información, deberán firmar un acuerdo de confidencialidad donde se comprometen a tratar la información de forma reservada y segura.

Los proveedores podrán tener acceso a los ambientes requeridos para labores de mantenimiento y soporte con previa autorización de la Dirección de TIC y bajo la supervisión y acompañamiento de esta área.

Los proveedores no podrán contar con usuarios para acceder directamente a las aplicaciones y bases de datos. Si es necesario, el acceso debe realizarse a través de un usuario interno autorizado para esto, que supervisará y controlará el acceso a estas.

Artículo 8: Adquisición e implementación de software

Cuando el usuario requiera instalar algún programa en su equipo de cómputo, deberá solicitarlo a mesa de ayuda y solo se permitirán aquellos con la licencia correspondiente y justificados para las actividades descritas en sus funciones.

Parágrafo 1: La descarga, uso o distribución de software sin la licencia correspondiente será responsabilidad del usuario y se sancionará conforme a la normatividad de la Universidad y leyes aplicables.

Parágrafo 2: La adquisición e implementación de programas y aplicaciones para la Universidad deberá estar avalada por el área de TIC, para garantizar que cumplan con los estándares de seguridad requeridos.

Artículo 9: Uso de computadores personales

El área TIC proporciona a cada empleado administrativo y profesor de planta un computador para desarrollar sus funciones, por lo que se prohíbe usar computadores personales para ello.

Parágrafo: La persona que por algún motivo tenga autorización para usar su computador personal para el desarrollo de sus funciones, debe firmar una carta de compromiso sobre el uso adecuado de este en las instalaciones de la EIA y cumplir mínimo con las siguientes medidas de seguridad:

a) Establecer una contraseña o patrón de desbloqueo de tipo biométrico.
b) Activar la opción de bloqueo automático por inactividad en el equipo.
c) Instalar solo programas de fuentes oficiales y que cuenten con licencia.
d) Tener instalada una herramienta de antivirus.
e) Tener el dispositivo y sus programas actualizados.
f) Almacenar la información institucional en la nube corporativa de OneDrive.

Artículo 10: Responsabilidades de los usuarios

a) Cada usuario de los sistemas de información de la Universidad es responsable de la seguridad y buen estado de los activos de información mediante un uso correcto de estos, siempre según sus atribuciones profesionales y académicas.
b) Las personas que realicen tratamiento de información de la Universidad que no sea pública, deben darle un manejo estrictamente reservado y confidencial, que salvaguarde la propiedad de la Universidad y se dé cumplimiento con la política de tratamiento de datos personales de la EIA.
c) Cualquier integrante de la Universidad en el desarrollo de sus actividades deberá:
    I. Cumplir y hacer cumplir esta política.
    II. Promover entre los integrantes de la comunidad universitaria conocimientos y conciencia de la importancia de las medidas de control de la seguridad de la información.
    III. Adoptar las medidas necesarias y adecuadas para el uso responsable de los activos de información utilizados en el ejercicio de sus funciones.
    IV. Participar en la capacitación y actualización de seguridad de la información y cualquier otra forma de enseñanza y entrenamiento que se considere pertinente.
d) Los empleados de la Universidad no deberán almacenar archivos con información institucional en el almacenamiento local de su equipo, estos se deberán guardar en la nube corporativa de OneDrive para su seguridad y protección.
e) Los usuarios deben reportar al área de TIC cualquier riesgo o amenaza que pueda identificar que afecte la seguridad de la información, como puede ser suplantación de identidad, robo de información, virus, entre otros.
f) El usuario es responsable de acatar las normas de Habeas Data de acuerdo con el artículo 15 de la Constitución Política de Colombia, la ley 1581 de 2012, la resolución 1377 de 2013 y las demás disposiciones que las modifiquen y complementen. Es importante tener en cuenta que se entiende por información privada aquellos datos de naturaleza íntima que se encuentra en el ámbito propio del sujeto, para acceder a ella se requiere autorización del titular o de

una autoridad judicial competente; y por información sensible aquellos datos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, así como los datos de niños niñas y adolescentes.

Artículo 11 Excepciones de Responsabilidad

Algunos usuarios pueden estar exentos de responsabilidad o de seguir alguno de los lineamientos enumeradas en este documento, debido a la responsabilidad de su cargo o a situaciones particulares. Estas excepciones deben ser solicitadas formalmente en un requerimiento en https://ayudame.eia.edu.co/ y aprobadas por la Dirección de TIC.

Artículo 12: Faltas graves

Constituyen faltas graves que atentan en contra de la seguridad de la informacióny podrán ser causal de sanción las siguientes:

a) Realizar actividades de intercepción o revelación de alguna comunicación digital
b) Generar con dolo o culpa grave algún tipo de incidente de ciberseguridad
c) Comercializar información propiedad de la institución.
d) Divulgar información reservada o confidencial propiedad de la Universidad o de terceros pertenecientes a grupos de interés.

Parágrafo 1: El desconocimiento de esta política por parte del usuario, no lo exime de las responsabilidades y sanciones a que se haga acreedor en términos de la normatividad de la Universidad vigente y demás disposiciones que en materia de seguridad de la información se señalen para tal efecto.

Parágrafo 2: La incursión en cualquiera de las conductas anteriormente mencionadas se considerará como incumplimiento al contrato (de trabajo, prestación de servicios, etc) y podrá dar lugar a la terminación con justa causa del mismo.

Artículo 13: Proceso disciplinario:

Una vez esclarecidos los hechos podrá darse inicio al proceso disciplinario sin perjuicio de los procesos judiciales a los que hubiere lugar, cuando el usuario que vulneró los términos de esta política ostente la calidad de profesor, investigador, empleado administrativo o de servicios el proceso se adelantará por la Jefatura de Gestión Humana, en caso de que se trate de un estudiante se acudirá al Consejo Académico.

Artículo 14: Sanciones

El usuario que incumpla las medidas de control para la seguridad de la información física o lógica establecidas en esta política podrá ser sancionado según la normatividad de la Universidad y las leyes aplicables. En caso de presentarse conductas que vulneren la seguridad de la información, la investigación del caso estará a cargo del Comité de Seguridad de la Información, de encontrarse que la conducta se dio por dolo, culpa grave, negligencia, o descuido se dará traslado a la instancia competente para iniciar el proceso disciplinario.

Parágrafo: La Universidad se reserva el derecho a ejercer las acciones legales para la protección y defensa de sus legítimos intereses en aquellos supuestos de hecho no contemplados en esta política, que pudieran ser de la competencia del Código Penal o cualquier otra legislación aplicable.

Artículo 15: Comité de ciberseguridad.

El Rector, mediante resolución rectoral nombrará a los integrantes del Comité de Ciberseguridad con el fin de fortalecer y mantener la estrategia de ciberseguridad para la protección de la información digital e

infraestructura tecnológica de la institución; serán responsabilidades de este Comité:

a) Desarrollar y mantener una estrategia de ciberseguridad que alinee los objetivos de seguridad con los objetivos empresariales. Esto incluye la creación y revisión de políticas de seguridad, estándares y procedimientos.
b) Identificar y evaluar los riesgos de seguridad cibernética que enfrenta la institución. Esto puede implicar el análisis de vulnerabilidades, amenazas y la evaluación de los impactos potenciales.
c) Establecer un plan de respuesta a incidentes que permita a la institución reaccionar de manera efectiva ante eventos de seguridad cibernética, minimizando daños y restaurando la operatividad normal.
d) Promover la educación y concienciación sobre ciberseguridad entre la comunidad interna de la EIA para reducir el factor humano como una fuente de vulnerabilidades.
e) Monitorear la infraestructura y los sistemas para detectar y responder a actividades sospechosas. Esto incluye la definición de herramientas de seguridad, como firewalls, sistemas de detección de intrusiones y sistemas de prevención de pérdida de datos.
f) Analizar las últimas tendencias y tecnologías en ciberseguridad y evaluar su aplicabilidad en la institución.
g) Vigilar que los proveedores y terceros cumplan con los estándares de seguridad cibernética establecidos.
h) Comunicar de manera efectiva las políticas, procedimientos e incidentes de seguridad cibernética a los grupos de interés.
i) Regularmente, evaluar la eficacia de las medidas de seguridad implementadas y buscar formas de mejorar la postura de ciberseguridad de la organización.
j) Adelantar la investigación sobre las posibles faltas graves contenidas en el presente documento.

Artículo 16. Vigencia

Esta política de seguridad estará vigente desde su aprobación y publicación y deberá ser revisada y actualizada por el Comité de Ciberseguridad anualmente o cuando se presenten cambios o eventualidades que así lo exijan.**Aprobado mediante resolución rectoral 171 del 4 de abril de 2024.**