0606
08-10-2020 12:06:38
Radicador: LUIS FELIPE ROSSO RICAUTE

RESOLUCIÓN No.0606
DEL 08-10-2020

“POR LA CUAL SE ESTABLECEN LINEAMIENTOS SOBRE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN DE LA INSTITUCIÓN UNIVERSITARIA DE ENVIGADO”.

LA RECTORA DE LA INSTITUCIÓN UNIVERSITARIA DE ENVIGADO, en uso de sus atribuciones legales y estatutarias, en especial por las conferidas en la ley 30 de 1992, el Acuerdo Estatutario del Consejo Directivo 013 del 26 de mayo de 2016, Ley 1437 de 2011, Ley 1341 de 2009, Decreto 2573 de 2014, Decreto 1078 de 2015, Decreto 1008 de 2018 y,

CONSIDERANDO

1. Que la ley 1341 de 2009 en el numeral 8, del artículo 2, establece que el Gobierno Nacional fijará los mecanismos y condiciones para garantizar la masificación de Gobierno en línea, con el fin de lograr la prestación de servicios eficientes a los ciudadanos, así mismo, la citada ley determinó que es función del Estado de intervenir en el sector de las TIC, con el fin de promover condiciones de seguridad de servicio al usuario final, incentivar acciones preventivas y de seguridad informática y de redes para el desarrollo de dicho sector, así como reglamentar las condiciones en que se garantizará el acceso a la información.
2. Que, el principio de Neutralidad Tecnológica, descrito en el artículo 6 de la Ley 1341 de 2009 manifiesta *"El Estado garantizará la libre adopción de tecnologías, teniendo en cuenta recomendaciones, conceptos y normativas de los organismos internacionales competentes e idóneos en la materia, que permitan fomentar la eficiente prestación de servicios, contenidos y aplicaciones que usen Tecnologías de la Información y las Comunicaciones y garantizar la libre y leal competencia, y que su adopción sea armónica con el desarrollo ambiental sostenible".*
3. Que dando cumplimiento con lo establecido por el Ministerio de Tecnologías de la Información y Las Telecomunicaciones (MINTIC), el gobierno nacional emitiò el Decreto 2573 de 2014, "*Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, y se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones*.
4. Que, el gobierno nacional emitió el Decreto 1078 de 2015, Único Sectorial *"Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".*
5. Que de acuerdo con el Decreto 1008 de 2018 *"Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones", en el articulo 2.2.9.1.2.1, se establece la estructura de la Polìtica de Gobierno Digital, como sus componentes y habilitadores transversales.*
6. Que la ley 1581 de 2012, constituye el marco general de la protección de los datos personales en Colombia.
7. Que el Decreto 1377 de 2013, art 3), con el fin de facilitar la implementación y cumplimiento de la Ley 1581 de 2012, reglamenta aspectos relacionados con la autorización del Titular de información para el Tratamiento de sus datos personales, las políticas de Tratamiento de los Responsables y Encargados, el ejercicio de los derechos de los Titulares de información, las transferencias de datos personales y la responsabilidad demostrada frente al Tratamiento de datos personales, este último tema referido a la rendición de cuentas.
8. Que la Super intendencia de Industria y Comercio y la Agencia Nacional de Defensa Jurídica del

Estado, emitieron la Circular 04 de septiembre de 2019, por la cual señalan los lineamientos que deben seguir las entidades públicas y particulares para el debido tratamiento de datos personales en sistemas de información interoperables. (*habeas data*).

9. Que por lo anterior, la Rectora,

RESUELVE

ARTÍCULO PRIMERO: Adoptar el modelo de Planes de Privacidad y Seguridad de la Información en la Institución Universitaria de Envigado, dentro del marco de su competencia constitucional y legal.

ARTÍCULO SEGUNDO: Establecer las Estrategias y Planes de Privacidad y Seguridad de la Información Institución Universitaria de Envigado, en desarrollo de los siguientes parámetros:

1. **ASPECTOS GENERALES.**

- Servir de guía respecto al uso responsable de la información y los recursos de tecnologías de información y comunicaciones y los deberes de los usuarios de la Institución Universitaria de Envigado en el uso de estos recursos.
- Hay que asegurar que el uso de la información y estos recursos cumpla con las leyes, normas y procedimientos de la Institución Universitaria de Envigado y la legislación de la República de Colombia.
- Proteger a la Institución Universitaria de Envigado de implicaciones legales, como consecuencia del uso indebido de la información y los recursos informáticos.
- Establecer claramente las responsabilidades que cada funcionario tiene en relación con el manejo de información y recursos tecnológicos.
- Crear una “Cultura de Seguridad y Autocontrol Informático” al interior de la Institución Universitaria de Envigado, para que los funcionarios tomen conciencia sobre la necesidad de proteger los equipos, el software y los datos, alineado con el Sistema de Gestión Integral.
- Proteger la información y sistemas de información contra cualquier forma de acceso no autorizado: utilización indebida, copia, publicación o modificación accidental o intencional de la información o software adquirido o desarrollado por la Institución Universitaria de Envigado con el fin de garantizar su confiabilidad, integridad y disponibilidad.
- Implementar mecanismos y controles que aseguren un efectivo registro, identificación y autenticación de los funcionarios de dichos servicios. Así mismo, implementar mecanismos y controles que aseguren el acceso bajo el principio del mínimo privilegio necesario para realizar las labores de cada funcionario, igualmente, implementar controles para una efectiva administración de usuarios y derechos de acceso.
- Garantizar la no repudiación de las transacciones implementando mecanismos de seguridad que permitan crear un ambiente de confianza entre los funcionarios públicos, los proveedores del servicio y la Institución Universitaria de Envigado.
- Proteger y manejar de manera responsable y segura los datos personales de los funcionarios y demás información enviada a través de los servicios de Gobierno digital.
- Conservar los atributos de correcta y completa durante la transmisión, el procesamiento y el almacenamiento de la información que se recibe o se envía a través de los servicios de Gobierno digital.
- Asegurar la disponibilidad de los servicios bajo control de la Institución Universitaria de Envigado.
- Proteger los datos de los funcionarios contra pérdida por actos accidentales o intencionales o por fallas de los equipos.

- Proteger los servicios y sus activos de información relacionados contra ataques externos o internos.
- Mantener y proteger los registros de las transacciones electrónicas como evidencia para los requerimientos de las auditorías (internas o externas) y como mecanismo para establecer responsabilidades de los usuarios internos y externos.
- Estas políticas están dirigidas a los funcionarios, contratistas, proveedores que hagan uso de la información y los recursos tecnológicos de información de la Institución Universitaria de Envigado y son aplicables a los recursos de tecnologías de información y comunicaciones y en general a todo equipo que sea conectado a la red Corporativa, o que tengan cualquier interacción con la infraestructura e información de la Institución Universitaria de Envigado.
- Los funcionarios se harán responsables por los perjuicios causados a la información y recursos de tecnología de información de la Institución Universitaria de Envigado, y por el incumplimiento de las presentes Políticas de Uso de la Tecnología y Seguridad de Información.

2. POLITICAS DE USO Y SEGURIDAD DE INFORMACIÓN.

2.1 Gestión de Activos de Información.

Los activos de información que son propiedad de la Institución Universitaria de Envigado son entregados para su uso, operación o custodia al personal a quien se aplica esta reglamentación, de acuerdo a las funciones específicas y necesidades derivadas de las actividades que deban realizar, sin que esto altere en ningún momento la propiedad de los mismos que seguirá estando a nombre de la Institución Universitaria de Envigado, aunque dentro de las funciones específicas se nombre dentro de la cadena de custodia u operación un propietario de cada activo de información. Este nombramiento como propietario, se hará únicamente, con el fin de asignar las responsabilidades operativas y de custodia sobre los diferentes activos.

La Institución Universitaria de Envigado asegura el manejo adecuado de la información dentro y fuera de la organización, a través de la clasificación e identificación de esta y estableciendo niveles apropiados de protección de acuerdo con dicha clasificación.

2.2 Seguridad de información y recursos humanos.

La Institución Universitaria de Envigado incluye en las actividades de inducción y reinducción temas relacionados con la seguridad de información, de acuerdo con las responsabilidades de cada uno de los funcionarios, con el fin de reforzar el conocimiento sobre el comportamiento adecuado en el tema, reduciendo errores humanos o abusos en el manejo de la información y sistemas asociados.

La Institución Universitaria de Envigado implementa controles para hacer seguimiento a los cambios de estado laboral de los funcionarios y ajustar así los privilegios de acceso de éstos.

2.3 Control de acceso.

La Institución Universitaria de Envigado establece e implementa procedimientos formales para controlar la asignación de derechos de acceso a usuarios. Dichos procedimientos cobijan todas las etapas del ciclo de vida del usuario, desde su registro inicial hasta el bloqueo o la eliminación del registro a quienes no necesiten más acceso. Se brinda atención especial, donde sea apropiado, a la necesidad del control de asignaciones de accesos privilegiados que permitan superar los controles básicos de los sistemas.

2.4 Organización para la gestión de la seguridad de información.

La Institución Universitaria de Envigado cuenta con proveedores estratégicos en la Seguridad de la Información, con el objeto de cumplir y soportar las actividades de Seguridad de la Información.

La Institución Universitaria de Envigado ha definido la participación y responsabilidades de todos sus

trabajadores dentro del ambiente de seguridad en la organización, para la vigilancia y cumplimiento de las Políticas de Seguridad establecidas.

2.5 Seguridad en la operación.

La Institución Universitaria de Envigado ha definido controles que garantizan la apropiada operación tecnológica. Estos controles incluyen entre otros los siguientes procedimientos: copias de seguridad, recuperación de datos y reversión de cambios, administración de sistemas de antivirus, administración de usuarios y contraseñas, administración de acceso a los recursos, administración de acceso remoto, medición de desempeño y capacidad de los recursos tecnológicos.

La Institución Universitaria de Envigado ha implementado controles que permiten garantizar un adecuado seguimiento a los cambios efectuados a los activos críticos de tecnología de información.

Las conexiones remotas de la Institución Universitaria de Envigado de ninguna forma estarán activas en horarios 7x24, cada que se requieran se debe realizar una solicitud justificada especificando fecha de conexión, hora de conexión, y fecha de terminación, persona que se conectara, si es del caso, el servicio será habilitado por una semana, estas políticas aplican para funcionarios y proveedores tecnológicos, las solicitudes deben hacerse como mínimo 2 días hábiles de anticipación a la mesa de ayuda.

2.5.1 Contraseñas.

Para crear nuevas contraseñas la política de contraseñas es: Mínimo 8 caracteres y se deben cumplir al menos 3 de las cuatro condiciones siguientes:

1. Mayúsculas
2. Minúsculas
3. Números
4. Caracteres especiales
5. La Caducidad de las contraseñas es 45 días.

2.5.2 Creación cuentas de correo.

Creación cuenta de correo para usuarios administrativos:

El procedimiento para crear la cuenta de correo institucional para los empleados administrativos de planta, es el siguiente:

1. Al ingresar el empleado a la institución y realizarse los trámites correspondientes en la oficina de Talento Humano, esta dependencia debe enviar correo a la mesa de ayuda *Te asisto* con los datos del nuevo empleado (incluyendo su cuenta de correo personal), solicitando la creación de su cuenta de correo Institucional.
2. Desde la mesa de ayuda se asigna el caso a la persona de informática con permisos de administración de la plataforma de correo office 365 para su creación.
3. Desde la oficina de Informática se crea la cuenta de correo teniendo en cuenta la nemotecnia establecida para tal fin en empleados de planta administrativos, la cual es: (primer nombre) +(punto)+ (primer apellido) @iue.edu.co
4. La nueva cuenta de correo no debe quedar repetida con ninguna de las existentes, si esto ocurre se agregará la primera letra del segundo apellido y así sucesivamente hasta que quede diferente a todas las existentes.

Creación cuenta de correo para usuarios contratistas:

El procedimiento para crear la cuenta de correo institucional para los contratistas, es el siguiente:

1. Al realizarse los trámites correspondientes a la firma del contrato (acta de inicio) en la oficina

Asesora Jurídica, esta dependencia debe enviar correo a la mesa de ayuda con los datos del nuevo contratista (incluyendo su cuenta de correo personal), solicitando la creación de su cuenta de correo Institucional.

2. Desde la mesa de ayuda se asigna el caso a la persona de informática con permisos de administración de la plataforma de correo office 365 para su creación.
3. Desde la oficina de Informática se crea la cuenta de correo teniendo en cuenta la nemotecnia establecida para contratistas la cual es: (primer nombre) + (primer apellido)+(punto)+(cont)@iue.edu.co

Creación cuenta de correo para usuarios estudiantes:
El procedimiento para crear la cuenta de correo institucional para los estudiantes tanto de pregrado como de posgrado, es el siguiente:

1. Al realizarse los trámites correspondientes al proceso de matrícula, la oficina de Admisiones y Registro envía correo para la creación de cuentas de correo Institucional, con el listado de los estudiantes matriculados por programa a la oficina de informática, este listado debe incluir (nombre completo del estudiante, documento de identidad, programa y cuenta de correo personal)
2. La oficina de informática asigna el caso a la persona con permisos de administración de la plataforma de correo office 365 para su creación.
3. La creación de la cuenta de correo institucional se hace teniendo en cuenta la nemotecnia establecida para los usuarios estudiantes, la cual es: (primera letra del primer nombre) + (primera letra del segundo nombre, si lo tiene) + (primer apellido) @correo.iue.edu.co
4. Para los casos en que el correo ya exista y pertenezca a otro usuario, se agregará la (primera letra del segundo apellido) y se continúa agregando de a una letra del segundo apellido hasta que el correo no esté repetido con los existentes.
5. Para la creación de las cuentas de correo de estudiantes nuevos, las cuales representan un gran número de usuarios, se estableció un procedimiento de creación masiva de correo, tanto para la creación de la cuenta como para la notificación de los usuarios a sus correos personales.

En caso de que exista un funcionario con el mismo nombre y apellido se creará de la siguiente manera: primer nombre. primer apellido y seguido de la primera letra del segundo apellido

2.5.3 Software no licenciado.

En caso de que el área de informática encuentre en las estaciones de trabajo software no licenciado, podrá desinstalar el Software no autorizado o borrar los archivos que considere necesarios de los Computadores. Igualmente se notificará a la secretaria general para iniciar proceso a través de la unidad de control interno disciplinario. y/o Talento Humano, para que adelanten los procesos sancionatorios correspondientes. Se llevará un registro para controlar el número de incidentes.

2.5.4 Prácticas de seguridad Informática.
Docente que requiera utilizar las plataformas tecnológicas de producción para hacer laboratorios en temas de seguridad Informática deben solicitar la creación de los ambientes como mínimo 8 días de anticipación al área de Informática, sujeto aprobación.

2.6 Seguridad en comunicaciones.
La Institución Universitaria de Envigado ha definido claramente las responsabilidades para el manejo y operación de instalaciones de computadores de escritorio y redes, apoyadas por instrucciones operacionales apropiadas incluyendo procedimientos de respuesta en caso de incidentes donde sea apropiado.

La Institución Universitaria de Envigado presta atención especial al manejo de la seguridad en redes, se han establecido medidas especiales para proteger el paso de información sensible a redes de dominio público.
Todo equipo de cómputo que vaya a ser conectado a la red de Institución Universitaria de Envigado debe ser revisado por la parte técnica de la Oficina de Informática, la cual revisara si las condiciones del hardware y software están debidamente actualizadas, y no garantizan ningún peligro para la seguridad e integridad de la información y dispositivos conectados en la institución.
Los estudiantes y visitantes que atenten a la seguridad informática de la Institución Universitaria de Envigado responderán con sanciones legales, y disciplinarias de la decanatura.

2.7 Seguridad física.
La Institución Universitaria de Envigado suministra instalaciones de tecnología de información que brindan apoyo a actividades sensibles de la organización protegiéndolas físicamente contra el acceso no autorizado, daño o interferencia. Los equipos se alojan en áreas seguras, protegidas por un perímetro de seguridad definido, con controles a entradas. Los controles de seguridad física son apoyados por controles de seguridad que permiten minimizar riesgos de disponibilidad, actualmente se tienen cámaras de seguridad y es de estricto cumplimiento diligenciar planilla de actividades al ingresar al Data Center.
La Institución Universitaria de Envigado ha implementado controles para garantizar que cualquier dispositivo o componente tecnológico sea destruido en forma segura. Estos controles incluyen la apropiada autorización y destrucción de datos previa a la destrucción física, teniendo en cuenta las normas legales vigentes, Políticas RAE.

2.8 Adquisición, desarrollo y mantenimiento de sistemas.
La Institución Universitaria de Envigado ha implementado controles para que todas las actividades relacionadas con el desarrollo y mantenimiento de sistemas de información, aunque sea desarrollado por terceros, consideren la administración de los riesgos de seguridad.
El diseño y operación de los sistemas obedece a estándares de seguridad de la industria comúnmente aceptados y con todos los requerimientos contractuales y legislativos relevantes.
Toda compra o arrendamiento de aplicaciones o sistemas de información, trabajos de grado de estudiantes se deberán consultar las condiciones mínimas que exige la oficina de informática para aceptar dicho montaje el cual deberá estar regulado por condiciones no solo de funcionamiento sino también de seguridad, esta consulta deberá ser realizada antes de la contratación, instalaciones realizadas sin este consentimiento previo en cualquier caso serán responsabilidad de la dependencia contratante.
Toda aplicación que sea soportada en producción deberá tener su contrato de soporte de mantenimiento, documentación y sus respectivos manuales.
Antes del paso de la producción todo requerimiento debe ser aprobado por el líder funcional donde notificara a través de correo electrónico su aprobación.
Ningún proveedor debe ingresar a los servidores de producción sin previa autorización del administrador de la infraestructura tecnológica, en caso de requerirse debe solicitar acceso con previo acompañamiento del área de Informática.
En caso de migración a nuevos sistemas de información se debe incluir migrar la información de información, no se tendrá sistemas de información paralelos.

2.9 Relación con proveedores.
La Institución Universitaria de Envigado tiene un inventario de los proveedores con que se relaciona, cada año realiza control de calidad de estos.

2.10 Gestión de incidentes de seguridad.

La Institución Universitaria de Envigado ha implementado un procedimiento formal de reporte de incidentes de seguridad por parte de los funcionarios al grupo de tecnología y para su respectivo escalamiento a través de la mesa de ayuda que son escalados al encargado de seguridad.
Cualquier desarrollo o aplicación que se pretenda montar en la infraestructura tecnológica de la IUE, antes de ser puesta en producción se le deberá hacer un análisis de vulnerabilidades y en caso de encontrarse fallas y riesgos con la misma deberán ser mitigados, los controles deben ser tanto para ataques internos como externos. La oficina de Informática se reserva el derecho a montar dichas publicaciones hasta que considere que dichos sitios son realmente seguros.

2.11 Aspectos de seguridad de información en la gestión de continuidad de negocio.
La Institución Universitaria de Envigado ha definido los controles a partir del Plan para la Continuidad del Negocio con el fin de desarrollar y mantener procedimientos apropiados de recuperación para procesos y servicios esenciales, después de un desastre o falla significativa que afecte los servicios y localidades. Dicho plan incluye la identificación y reducción de riesgos provenientes de acciones premeditadas o accidentales contra servicios vitales.
Las salidas a producción de cambios, ajustes al software o solicitudes de acceso a los fines de semana deberán ser solicitados al menos con 24 horas de anticipación, se aclara que el permiso es valido por el fin de semana solicitado.

2.12 Servicio de Soporte.
La línea Mesa de Ayuda es un servicio integral que ofrece la posibilidad de gestionar y solucionar todas las posibles incidencias y atención de requerimientos relacionados a la tecnología de Información y plataformas tecnológicas. Solo se atienden las solicitudes registradas en la herramienta de Mesa de Ayuda.
Las solicitudes relacionadas con eventos audiovisuales deberán será colocadas como mínimo con dos días hábiles de anticipación previo al evento. se debe realizar la solicitud a la mesa de ayuda especificando todas las necesidades..
Las solicitudes de arreglo de equipos de docentes que están fuera la Institución universitaria de envigado deberán ser llevados al área de soporte y se dará respuesta dentro de las próximas 24 horas (siempre y cuando estos sean propiedad de la Institución Universitaria de envigado).
Todo funcionario de la Instrucción universitaria es responsable de la custodia de la información.
Equipos personales de los funcionarios de la Institución Universitaria de Envigado no son revisados ni reparados por personal del área de informática.
La Institución Universitaria de Envigado ha implementado controles para garantizar la seguridad de la información de aquellos equipos que eventualmente son remitidos a los proveedores para garantía. Este control comprende acuerdos de confidencialidad de información con los terceros.

3. MEDIDAS DISCIPLINARIAS.

al incumplimiento de los lineamientos le aplican las sanciones disciplinarias que se especifican en la Ley 734 de 2002 Código Único Disciplinario, o las normas vigentes en relación con los procesos disciplinarios.

"Artículo 34. *Deberes. Son deberes de todo servidor público:*

(...)

Todo servidor público debe responder por la conservación de los equipos, muebles y bienes confiados a su custodia o administración y rendir cuenta oportuna de su utilización.

Utilizar los bienes y recursos asignados para el desempeño de su empleo, cargo o función, las facultades que le sean atribuidas, o la información reservada a que tenga acceso por razón de su función, en forma exclusiva para los fines a que están afectos.

(...)"

Es responsabilidad de todo funcionario salva guardar su información, no es responsabilidad del área de informática, esta debe ser salvaguardada en one drive.

***"Artículo 35.** Prohibiciones. A todo servidor público:*

(...)

Ocasionar daño o dar lugar a la pérdida de bienes, elementos, expedientes o documentos que hayan llegado a su poder por razón de sus funciones.

(...)"

Son conductas motivo de sanciones y/o procesos disciplinarios, las siguientes faltas o conductas:

4. Prestar el usuario de red para permitir el acceso de personas no autorizadas a aplicativos que requieren autorización de uso.
5. Instalar Software no autorizado por Informática, actividad que incurre en sanciones.
6. Usar indebidamente, modificar o alterar información confidencial, restringida, importante o crítica.
7. Realizar alguna acción que pueda causar daño físico en los equipos o infraestructura (destrucción, sustracción, traslados no autorizados, y demás.)
8. Realizar ninguna instalación de equipos de comunicaciones para el acceso remoto (Módems, ADSL, RDSI, Reuters, y otros.) e intercambio de información (rutas, redes) entre sistemas de la Red del Institución Universitaria de Envigado y el exterior, salvo que hayan sido autorizados por la Oficina de Informática.
9. Realizar alguna actividad que suponga violar la privacidad de los datos y el trabajo de los otros usuarios, como pruebas de pruebas de hacking, o ataques informáticos contra la Institución Universitaria de Envigado.
10. Usar las herramientas informáticas de la entidad, para fines lucrativos o personales.
11. Hacer mal uso de recursos informáticos como el correo o el Internet, enviando información ilegal, discriminatoria, ofensiva, agresiva, intimidatoria u obscena a otras personas o entidades, publicidad, ventas, acceder a páginas con contenido pornográfico, violento despectivo o que se considere atente contra la moral.
12. Está prohibido ingresar a sitios como: páginas de contenido pornográfico, emisoras de radio y televisión, páginas de videos y películas online, redes sociales (Facebook, Twitter, y whatsapp otros), que no estén relacionados con temas institucionales.
13. Se prohíbe la transmisión o distribución de cualquier material discriminatorio, hostil, degradante o intimidatorio para cualquier persona o grupo de personas debido a su religión, género, orientación sexual, raza, etnia, edad o discapacidad.
14. Se prohíbe transmitir mensajes que revelen cuestiones personales o privadas relativas a cualquier persona y que puedan infringir los derechos de estas.
15. Es prohibido suplantar a otra persona a través del correo electrónico, hacer declaraciones falsas,

falsificar la identidad de alguna persona en los encabezados de los mensajes.

16. Se prohíbe transmitir información cuyo contenido sea ilegal, peligroso, invasor del derecho a la privacidad, pornográfico, ofensivo a terceros o violatorio de derechos de autor, marcas o patentes.
17. La información sensible no cifrada no debe ser enviada por correo electrónico.
18. Cuando se trate de alguna fecha especial, la Oficina de Comunicaciones será la única encargada de enviar masivamente los textos de conmemoración o felicitaciones a través del correo corporativo. En ciertos casos el área de Informática podrá enviar correos con los temas informáticos.
19. No se permite utilizar el correo electrónico, la publicación Web o cualquier otro medio de difusión electrónica de la información para realizar manifestaciones o adquirir compromisos en nombre de la Institución Universitaria de Envigado sin tener la competencia o autorización para ello.
20. Por política de seguridad en red de datos de una dependencia no se podrá acceder a la máquina de otra dependencia, acción que estará restringida, cuando se necesite compartir información con funcionarios de otras áreas, lo podrán realizar a través del servidor de archivo solicitando los permisos respectivos para ingresar a la carpeta de su interés, dichos permisos deben ser autorizados por el área correspondiente.
21. El intercambio de archivos en la red se hará a través de servidores destinados para tal fin no entre equipos de cómputo.
22. No está permitido el uso de programas que tengan como fin hacer rastreo de puertos, recolección de información trasmitida, monitorear comunicaciones, Establecer los servicios de DHCP y DNS, buscar vulnerabilidades en la red, servidores, computadoras y equipos de comunicaciones, ni falsificar la identidad de un usuario.
23. Los funcionarios no deben descargar software de cualquier sistema externo a la Institución Universitaria de Envigado.
24. Los usuarios finales no deben descargar software de Internet en ninguna circunstancia.
25. Está prohibido instalar aplicativos de uso temporal, sin la autorización de la mesa de ayuda o de la oficina de Informática.
26. Explícitamente se encuentran prohibidos TeamViewer, anydesk o herramientas similares de conexón remota Sql navigator (solo permitido en informática y con Autorización).
27. Está prohibido bajar de Internet música, videos, fotos, y juegos que no sean de interés laboral, juegos.
28. Está prohibido mover equipos sin autorización de la oficina de Informática.
29. Está prohibido la instalación de cualquier tipo de Software que no este licenciado por el Institución Universitaria de Envigado.
30. Está prohibido entrar a la red oscura de internet para realizar temas mal

4. EXCEPCIONES .

Las personas que por sus funciones necesiten tener habilitado servicios que están prohibidos en la presente resolución, estos deben de tener autorización de su jefe inmediato y ser aprobados por la Oficina de Informática.

5.NOTIFICACIÒN Y PUBLICACIÒN.

Estás directrices deben ser comunicadas a todo usuario que labore en la Institución Universitaria de Envigado y haga uso de la infraestructura tecnológica, en el caso de los contratistas, debe mencionarse el cumplimiento de estas directrices en el contrato que se suscriba con el mismo.

La presente Política se encontrará publicada en el Sistema de Gestión Integral.

6. VERIFICACIÒN

El cumplimiento de la presente política estará a cargo de la Oficina de Informática, la Oficina de Control Interno y la unidad de Control Disciplinario según sea el caso.
Todos los usuarios tienen la responsabilidad de notificar a la Oficina de Informática cualquier acción descubierta en relación con la violación de alguna de las políticas de seguridad descritas en este documento.
Las políticas tendrán una revisión periódica mínimo una vez al año para realizar actualizaciones, modificaciones y ajustes basados en las recomendaciones, sugerencias, cambios normativos y tecnológicos.

7. DEFINICIONES

Red profunda: es un espacio virtual al que no se puede entrar desde la Internet comercial, es un espacio oculto en el que hay 'libertad' de acceso a todo tipo de contenido.

Activo: En relación con la seguridad de la información, se refiere a cualquier información o sistema relacionado con el tratamiento de esta que tenga valor para la organización. Según [ISO/IEC 27000:2012]: Cualquier cosa que tiene valor para la organización.

Control: Forma de gestionar el riesgo, incluyendo políticas, procedimientos, guías, prácticas o estructuras organizacionales, las cuales pueden ser de naturaleza administrativa, técnica, de gestión o legal [ISO/IEC 27000:2012].

Seguridad de la información: Según [ISO/IEC 27000:2012]: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.

Incidente: Según [ISO/IEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Política de seguridad: Documento que establece el compromiso de la Oficina y el enfoque de la organización en la gestión de la seguridad de la información. Según [ISO/IEC 27002:2005]: intención y Oficina general expresada formalmente por la Dirección.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.

Análisis de riesgos: Según [ISO/IEC 27000:2012]: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
Gestión de riesgos: Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos. Según [ISO/IEC 27000:2012]: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados. Según [ISO/IEC 27000:2012]: Característica o propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

Amenaza: Según [ISO/IEC 27000:2012]: causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO/IEC 27000:2012]: debilidad de un activo o conjunto de activos que puede ser explotado por una o más amenazas.

Disponibilidad: Acceso a la información y los sistemas de tratamiento de esta por parte de los usuarios autorizados cuando lo requieran. Según [ISO/IEC 27000:2012]: característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISO/IEC 27000:2012]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.

SGSI: Sistema de Gestión de la Seguridad de la Información. Según [ISO/IEC 27001:2005]: la parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos).

Servicio o aplicación: Programa o conjunto de programas diseñados para la realización de unas tareas concretas. Los servicios están destinados principalmente para apoyar los procesos de negocio de la entidad. Por ejemplo, correo electrónico, internet, Finanzas, Impuestos, etc.

Cuenta de acceso: Identificación y contraseña a través de la cual el usuario accede a un servicio o aplicación. Las cuentas de acceso son aprobadas por los jefes de las Dependencias y suministradas por la Oficina de Informática y están sujetas a la disponibilidad de licencias adquiridas por la Alcaldía.

Archivos: Conjunto de datos o instrucciones que se almacenan en el Disco Duro y/o dispositivos de almacenamiento con un nombre que los identifica.

Equipos de cómputo: incluye computadores de escritorio, portátiles, tabletas, dispositivos móviles, servidores.

ARTÌCULO TERCERO: el contenido de estos lineamientos será comunicados a todo el personal Docente, Administrativo y Contratista de la Institución Universitaria.

Dado en el Municipio de Envigado, **08-10-2020**

PUBLÌQUESE Y CÚMPLASE

BLANCA LIBIA ECHEVERRI LONDOÑO
RECTOR DE INSTITUCIÓN UNIVERSITARIA
RECTORÍA

JUAN FELIPE ACOSTA GONZALEZ

0606
08-10-2020 12:06:38
Radicador: LUIS FELIPE ROSSO RICAUTE

SECRETARIO GENERAL DE INSTITUCIÓN UNIVERSITARIA
SECRETARÍA GENERAL

Proyectó: LUIS FELIPE ROSSO RICAUTE

Revisó: JOSE LEONARDO ZAPATA VERGARA

Aprobó: RAINIERO ALEXANDER GONZALEZ CASTRO