UNIVERSIDAD EAN
ACREDITADA INSTITUCIONALMENTE
EN ALTA CALIDAD
Res. nº. 12773 del Mineducación
19/09/13, vigencia 19/09/17
Vigilada Mineducación

MANUAL DE SEGURIDAD DE LA INFORMACIÓN
V. 3

ELABORADO POR:

GERENCIA DE INNOVACIÓN Y DESARROLLO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Bogotá, 2017

CONTROL DE VERSIONES

Versión	Fecha	Descripción
0	Junio 2014	Creación del documento
1	Noviembre 2015	Cambio de estructura organizacional
2	Enero 2016	Resultado Consultoría Habeas Data
3	Junio 2017	• Actualización lineamientos de: · Seguridad para el teletrabajo · Seguridad para los repositorios institucionales. · Seguridad para el correo electrónico · Seguridad para la administración de cuentas y contraseñas de usuario · Seguridad para la gestión de incidentes · Seguridad para proveedores o terceros · Seguridad para la adquisición de servicios de cloud computing y hosting · Administración de datos personales (habeas data) · Roles y responsabilidades

ACUERDO DE CONFIDENCIALIDAD

El documento está catalogado como de uso interno (Exclusivo para la Universidad EAN).

CONTENIDO

CONTROL DE VERSIONES 2
PRESENTACIÓN Y BASE LEGAL 7
CAPÍTULO I - OBJETIVOS Y ALCANCE 8
OBJETIVOS 8
ALCANCE 8
MEDIDAS DE SEGURIDAD 8
CAPÍTULO II - LINEAMIENTOS 9
LINEAMIENTOS DE SEGURIDAD PARA EL TELETRABAJO 9
Descripción 9
Acceso a la red de datos 9
Almacenamiento de información 10
Acceso al sistema de telefonía 10
Acceso a servidores de archivos 10
Acceso a los sistemas de información 11
Uso de hardware y software 11
Criterios de confidencialidad de documentos 12
LINEAMIENTOS DE SEGURIDAD PARA EL CORREO ELECTRÓNICO 12
Descripción 12
Infraestructura tecnológica 12
Aspectos generales 13
Administración del correo electrónico 13
Creación, borrado o inactivación de las cuentas de correo electrónico 13
Acceso al servicio de correo electrónico 16
Uso del correo electrónico 16
LINEAMIENTOS DE SEGURIDAD PARA EL USO DE MEDIOS DE ALMACENAMIENTO EXTRAÍBLES O REMOVIBLES 18
Descripción 18
Uso de medios de almacenamiento extraíbles 18
LINEAMIENTOS DE SEGURIDAD PARA COPIAS DE RESPALDO 19
Descripción 19
Restauración de copias de respaldo 20
Respaldo de servicios alojados en internet o en sitios alternos de proveedores de servicios 20
LINEAMIENTOS DE SEGURIDAD PARA LOS REPOSITORIOS INSTITUCIONALES 21
Descripción 21
Uso de los repositorios institucionales 21
LINEAMIENTOS DE SEGURIDAD PARA LA ADMINISTRACIÓN DE CUENTAS Y CONTRASEÑAS DE USUARIO 23
Descripción 23
Administración de cuentas 23
Cuentas normales 23
Cuentas privilegiadas 24
Cuentas de procesos 24
Cuentas de proveedores que prestan servicios de tecnología 25
Administración de contraseñas 25
Para cuentas normales y proveedores que prestan servicios de tecnología 25

Para cuentas privilegiadas 25
Uso de cuentas y contraseñas de usuario 25
Desvinculación o cambio de rol de colaboradores y terceros 26
LINEAMIENTOS DE SEGURIDAD PARA LA CLASIFICACIÓN, RECICLAJE Y/O DESTRUCCIÓN DE LA INFORMACIÓN 26
Descripción 26
Información sensible o confidencial 27
Información pública 27
Administración de la información sensible o confidencial 27
Administración del respaldo de la información 28
Uso de la información (Clasificación, Reciclaje y/o Destrucción de la información) 28
LINEAMIENTOS DE SEGURIDAD PARA LA GESTIÓN DE INCIDENTES 29
Descripción 29
Tipos de incidentes 29
Reporte gestión de incidentes 30
Gestión de incidentes 30
LINEAMIENTOS DE SEGURIDAD PARA INGRESO AL DATACENTER 31
Identificación y autenticación 31
Administración del datacenter 31
Acceso 32
Monitoreo y control 32
Registro de las actividades y acciones del personal 32
Normas de Seguridad 33
LINEAMIENTOS DE SEGURIDAD PARA LA INFRAESTRUCTURA TECNOLÓGICA 33
Mantenimiento preventivo y correctivo 33
Infraestructura del Datacenter 33
Renovación tecnológica y reposición de equipos 34
Asignación de equipos de cómputo a colaboradores 34
Préstamo de equipos a estudiantes y docentes 35
Equipos de cómputo de contratistas y proveedores 35
Equipos que ingresan a la Universidad EAN 36
Instalación de Software 36
Instalación o retiro de hardware 36
Información almacenada en la infraestructura tecnológica 37
Acceso a la Red de datos 37
Navegación en Internet 38
LINEAMIENTOS DE SEGURIDAD PARA PROVEEDORES O TERCEROS 38
Descripción 38
Lineamientos de ingreso de equipos portátiles y escritorio remoto 38
Lineamientos generales 38
LINEAMIENTOS DE SEGURIDAD PARA LA ADQUISICIÓN DE SERVICIOS DE CLOUD COMPUTING Y HOSTING 39
Descripción 39
Lineamientos Generales 40
LINEAMIENTOS DE SEGURIDAD PARA PROYECTOS 42
Descripción 42
Lineamientos generales 42
LINEAMIENTOS DE SEGURIDAD PARA FIRMA DIGITAL 43

Descripción 43
Lineamientos generales 43
LINEAMIENTOS ADMINISTRACIÓN DE DATOS PERSONALES (HABEAS DATA) 43
Medidas de seguridad comunes 43
Gestión de documentos y soportes 44
Control de acceso 44
Ejecución del tratamiento fuera de los locales 44
Bases de datos temporales, copias y reproducciones 44
Medidas de seguridad para bases de datos no automatizadas 45
1. Almacenamiento 45
3. Custodia de documentos 45
Auditorías 46
Archivo de documentos 46
Acceso a los documentos 46
Medidas de seguridad para bases de datos automatizadas 47
Identificación y autenticación. 47
Entrada y salida de documentos o soportes 47
Copias de respaldo y recuperación de datos personales. 47
Registro de acceso 48
Redes de comunicaciones 48
Bases de datos y sistemas de información 48
Medidas para el transporte, destrucción y reutilización de documentos y soportes 49
CAPÍTULO III. ROLES Y RESPONSABILIDADES 50
COLABORADORES, DOCENTES Y ESTUDIANTES 50
PROCESOS 50
Gerencia de Desarrollo Humano 50
Gerencia de Innovación y Desarrollo de TIC 50
LÍDERES SISTEMAS DE INFORMACIÓN 50
Líder funcional: 50
Líder técnico: 50
COMITÉ DE SEGURIDAD DE LA INFORMACIÓN Y GESTIÓN DOCUMENTAL 50
RESPONSABILIDADES PARA COLABORADORES 50
DISPOSICIONES 51
CAPÍTULO IV. DEFINICIONES 52
BIBLIOGRAFÍA 56

PRESENTACIÓN Y BASE LEGAL

La Universidad EAN mediante el Acuerdo No. 060 de Septiembre 17 de 2009, adopta la Política de Seguridad Informática, en donde se reconoce el valor y la importancia de la información como activo de la organización, para lo cual propone desarrollar acciones que atiendan las buenas prácticas de seguridad y adoptar los controles y medidas necesarias para dar protección a los datos, siempre orientados a generar confiabilidad respetando la privacidad de la información de los diferentes grupos de interés.

En 2012, la Universidad EAN a través de la Gerencia de Innovación y Desarrollo de TIC formuló como objetivo estratégico la Seguridad de la Información, alineado con el Plan de Desarrollo Institucional. Igualmente, a través de la Resolución 059 del 5 de Julio de 2012 modifica el Comité de Archivo por el de Comité de Seguridad de la Información y Gestión Documental de la Universidad EAN, en donde se identifica la necesidad de formalizar las directrices y lineamientos para el uso de las Tecnologías de la Información y Comunicación, la promoción y aplicación de las buenas prácticas de seguridad de la información en la institución.

En este contexto y amparados por el Reglamento Interno de Trabajo de la Universidad EAN, 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 parcialmente la Ley 1581, la Ley 23 de 1982 que contiene las disposiciones generales y especiales que regulan la protección del derecho de autor en Colombia, el Decreto Numero 884 de 2012 que reglamenta la Ley 1221 de 2008 que promueve y regula el Teletrabajo, la Ley 1273 de 2009 por la cual se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”; la Universidad EAN construye este manual como una herramienta para garantizar el buen uso y la preservación de la infraestructura tecnológica, la información institucional y generación de mecanismos para realizar la protección de los datos de acuerdo a la normativa vigente, así como, minimizar los riesgos asociados a la ejecución de actividades mediadas por las Tecnologías de la Información y Comunicación.

El Manual de Seguridad es un documento interno de la Universidad de obligatorio cumplimiento para todo colaborador o persona que tenga relación con la Universidad EAN, con acceso a los sistemas de información y a las bases de datos.

Este manual debe ser sometido a permanente revisión y actualización siempre que se produzcan cambios en los sistemas de información, el sistema de tratamiento de datos, la organización o el contenido de la información de las bases de datos, que puedan afectar a las medidas de seguridad implementadas. Asimismo, el manual debe adaptarse en todo momento a la normativa legal en materia de seguridad de la información y de datos personales.

El incumplimiento de los lineamientos presentados en este manual por parte de colaboradores, estudiantes, docentes y terceros tendrá consecuencias de acuerdo al tipo de incumplimiento y estará sujeto a la legislación nacional, la normativa local y la normativa interna aplicable a la institución según lo indique la Universidad.

CAPÍTULO I - OBJETIVOS Y ALCANCE

OBJETIVOS

- Garantizar la confidencialidad, integridad y disponibilidad de la información institucional como activo de la organización, con la incorporación de buenas prácticas, preservación de la infraestructura tecnológica y normas de calidad aplicables a la gestión segura de las Tecnologías de la Información y la Comunicación.

- Garantizar la protección de los datos personales de los cuales es responsabilidad la Universidad EAN en sistemas de información, bases de datos, soportes y equipos empleados en el tratamiento de los datos, teniendo en cuenta la normativa interna vigente.

ALCANCE

Aplica para todos los colaboradores, estudiantes, docentes de planta y cátedra para cualquier modalidad educativa y de contratación, visitantes, proveedores externos que hagan uso de la información, sistemas de información y recursos informáticos de la universidad EAN.

MEDIDAS DE SEGURIDAD

Los sistemas de información, los recursos tecnológicos, las bases de datos son accesibles únicamente por las personas designadas por la Universidad EAN.

Los responsables de los datos de la Universidad EAN, se encargan de gestionar los permisos de acceso a los usuarios, el procedimiento de asignación y distribución que garantiza la confidencialidad, integridad y almacenamiento durante su vigencia, así como la periodicidad con la que se cambian.

A continuación, se enumeran y detallan los lineamientos y medidas de seguridad implementadas por La Universidad EAN.

CAPÍTULO II - LINEAMIENTOS

LINEAMIENTOS DE SEGURIDAD PARA EL TELETRABAJO

Los lineamientos de seguridad para el teletrabajo comprenden: descripción del servicio y conexión remota a la red de datos, acceso al sistema de telefonía, acceso a servidores de archivos, acceso a sistemas de información, almacenamiento de la información, uso de hardware y software. Podrán aplicarse teniendo en cuenta el rol desempeñado en la Universidad.

Descripción

La Universidad EAN ha adoptado modalidades de contratación de colaboradores en teletrabajo (Teletrabajadores), por lo tanto, se hace necesario establecer las condiciones técnicas y de seguridad sobre las cuales el teletrabajador accederá a los recursos, bases de datos personales y servicios de tecnología de la Universidad.

La Universidad EAN a través de la Gerencia de Innovación y Desarrollo de TIC proporcionará al Teletrabajador el equipo de cómputo para el desarrollo de sus actividades laborales. No está permitido el uso de equipos personales para el desarrollo de las actividades laborales asignadas por la Universidad.

El Teletrabajador solo puede acceder a los sistemas, aplicativos y servicios que le han sido aprobados en teletrabajo, en el horario laboral acordado con la institución.

Acceso a la red de datos

Para el desarrollo de las actividades en modalidad de Teletrabajo se puede requerir de una conexión remota a la red de datos de la Universidad EAN, a través de una VPN (Red Privada Virtual) que cumpla con requisitos mínimos para garantizar la integridad y confidencialidad en la transferencia de información. En caso que el colaborador no requiera hacer uso de los servicios descritos a continuación, no se hace necesario la asignación de una VPN, pero deberá apoyarse en las herramientas colaborativas dispuestas por la Universidad.

Para tales efectos la Gerencia de Innovación y Desarrollo de TIC instalará en el equipo de cómputo asignado por la Universidad EAN al Teletrabajador, el software y las credenciales de acceso requeridas para el establecimiento de la VPN. Bajo ninguna circunstancia se instalarán dichas herramientas en equipos de propiedad del Teletrabajador.

Para el establecimiento de la conexión remota se tienen en cuenta los siguientes aspectos:

- Evitar establecer conexiones a redes inalámbricas desconocidas o que estén habilitadas sin seguridad, es decir, que no solicite claves de ingreso. El riesgo aparece cuando el punto de acceso está abierto intencionalmente con un propósito malicioso, para obtener información de forma indebida por parte de una persona no autorizada.
- Cambiar periódicamente las credenciales para el establecimiento de la VPN. Dichas solicitudes se registran en la mesa de servicio de soporte de la Gerencia de Innovación y Desarrollo de TIC.
- Las credenciales asignadas para el establecimiento de la VPN son de uso personal e intransferible, por tanto, no se comparten o divulgan. Su uso inadecuado es responsabilidad exclusiva del Teletrabajador.

Almacenamiento de información

- Usar el repositorio institucional asignado por la Universidad EAN para guardar la información, en caso de almacenarla en los discos locales del equipo asignado, se debe utilizar la partición protegida y descargar la información en los repositorios institucionales posteriormente, para prevenir qué ante una situación de hurto del equipo de cómputo, se pierda y exponga la información de la institución.
- La Gerencia de Innovación y Desarrollo de TIC, instala una herramienta de cifrado de disco para proteger la información sensible que se encuentre almacenada en el equipo de cómputo. El Teletrabajador se encuentra en la obligación de hacer uso de esta para proteger la información de trabajo que pueda almacenar a nivel local en el equipo de cómputo asignado.
- La conexión de medios extraíbles al equipo del Teletrabajador como (USB, Unidades CD/DVD, Discos externos, entre otros, son monitoreadas y eventualmente podrá ser restringida de acuerdo con los lineamientos que la Universidad EAN disponga para evitar la fuga de información y garantizar la confidencialidad y protección de los datos. En los equipos de cómputo de los Teletrabajadores no se permite el almacenamiento de archivos de música, videos y cualquier otro formato o información de carácter personal, salvo aquellos cuyo uso o almacenamiento sea para ejecutar labores propias de la Universidad EAN. La Gerencia de Innovación y Desarrollo de TIC está facultada para eliminar archivos que no cumplan con los propósitos de la Universidad EAN.
- En caso de requerir documentos físicos o información en dispositivos de almacenamiento extraíbles (como USB, CD, discos duros externos, entro otros) para el desarrollo de su actividad, el Teletrabajador es responsable por la custodia y preservación de los mismos; se recomienda no dejarlos expuestos a terceros no autorizados, guardarlos bajo llave y en un lugar seguro. Tener en cuenta el tratamiento de datos personales de acuerdo a este manual.

Acceso al sistema de telefonía

Para el desarrollo de las actividades en modalidad de Teletrabajo, a cada Teletrabajador se le asigna, si es necesario, una extensión telefónica y un software de telefonía que se conecta y registra con los servidores de telefonía de la Universidad EAN; esta conexión se establece a través de la VPN. Para la comunicación telefónica se tienen en cuenta los siguientes aspectos:

- Los perfiles de marcado para llamadas a larga distancia y operadores de telefonía celular, son asignados siempre y cuando estos sean autorizados por el líder del proceso, al que pertenece el colaborador, quien deberá realizar la solicitud a través de la mesa de servicio o software de gestión de solicitudes a la Gerencia de Innovación y Desarrollo de TIC.
- Las credenciales asignadas para la conexión al sistema de VPN son de uso personal e intransferible, por tanto, no se comparten o divulgan.
- Evitar el intercambio de información en la comunicación telefónica con personas ajenas a la Universidad, puesto que esta herramienta facilita la aplicación de técnicas de ingeniería social para obtener información sensible de la institución.

Acceso a servidores de archivos

El acceso a servidores de archivos en modalidad de Teletrabajo se asigna de acuerdo a los perfiles autorizados para realizar las labores propias del cargo, por lo tanto, se debe tener en cuenta los siguientes aspectos:

- Velar por la seguridad y confidencialidad de la información contenida en los servidores de archivo.
- Evitar compartir el equipo de cómputo con personas no autorizadas, para que no exista un acceso no permitido a la información y a los sistemas de información de la Universidad.

Acceso a los sistemas de información

El acceso a los sistemas de información en modalidad de Teletrabajo se asigna de acuerdo a los perfiles autorizados para realizar las labores propias del cargo, considerando los siguientes aspectos:

- Acceder con las credenciales asignadas al Teletrabajador para acceder a los sistemas de información.
- Las credenciales asignadas para el acceso a los sistemas de información, son de uso personal e intransferible, por tanto, no se comparten o divulgan.
- Salvaguardar la información contenida en los diferentes sistemas de información a los que se tenga acceso autorizado, evitando compartir el equipo de cómputo con personas ajenas.

Uso de hardware y software

El hardware y software otorgado por la Universidad EAN, para el desarrollo de la modalidad de Teletrabajo se utiliza únicamente para llevar a cabo las actividades laborales asignadas por la Universidad. Por lo anterior se tienen en cuenta los siguientes aspectos:

- Evitar abrir correos electrónicos, descargar o ejecutar archivos de los cuales no se conozca su procedencia. Este tipo de práctica es una de las principales fuentes de virus o programas maliciosos, que pueden generar un daño irreversible al computador y afectar la confidencialidad de la información de la Universidad.
- Evitar abrir y ejecutar ventanas emergentes, barras de herramientas, programas, enlaces desconocidos; estos pueden conducir a sitios de suplantación web para capturar datos que pueden afectar la disponibilidad, integridad y confidencialidad de la información de la Universidad.
- Evitar instalar programas ajenos a los autorizados por la Universidad o que no correspondan al desarrollo normal de las actividades asignadas. El único proceso autorizado para instalar software en los equipos de cómputo institucionales es la Gerencia de Innovación y Desarrollo de TIC.
- La Gerencia de Innovación y Desarrollo de TIC, instala una herramienta de antivirus para proteger el equipo de amenazas de virus, es recomendable que el Teletrabajador compruebe el correcto funcionamiento del mismo, y si presenta alguna falla se reportan a la mesa de servicio de soporte.

El Teletrabajador es responsable por los daños ocasionados a los equipos de cómputo generados por mal uso de los mismos, por lo tanto, se tienen en cuenta las siguientes recomendaciones:

- Evitar exponer el equipo de cómputo en sitios públicos como centros comerciales o campos abiertos.
- Hacer uso del equipo de cómputo asignado únicamente en el lugar de teletrabajo aprobado por la Universidad de acuerdo a la visita realizada por la Gerencia de Gestión del Desarrollo Humano. Este espacio debe contar con las condiciones de seguridad física para proteger los recursos de la institución.
- Evitar exponer el equipo de cómputo en zonas donde exista humedad.
- Evitar golpes y consumir líquidos mientras se desarrollan actividades de Teletrabajo ya que existe el riesgo de avería parcial o total del equipo de cómputo.

- Evitar utilizar o dejar el equipo de cómputo donde pueda sufrir calentamiento, esto generaría daño en la fuente y a nivel general.
- En caso de pérdida o hurto del equipo de cómputo, el Teletrabajador debe informar inmediatamente a la mesa de servicio de soporte de la Gerencia de Innovación y Desarrollo de TIC, la Vicerrectoría Financiera y la Gerencia de Desarrollo humano.
- Cualquier software adicional al instalado en el momento de entrega del equipo, se notifica al personal de la Gerencia de Innovación y Desarrollo de TIC para efectos de inventario.
- No está autorizado ningún tipo de modificación en el hardware.
- El Teletrabajador debe verificar el estado en el cual es entregado el equipo en el momento de su recepción. Para ello se genera un formato de entrega que debe ser firmado indicando conformidad en la entrega y recepción por parte del Teletrabajador y la Gerencia de Innovación y Desarrollo de TIC.

Criterios de confidencialidad de documentos

El Teletrabajador debe dar cumplimiento a los lineamientos de seguridad de la información asociados a la clasificación, etiquetado y manejo de documentos e información y bases de datos personales, considerando los siguientes criterios de confidencialidad de documentos:

- **Sensible o confidencial:** se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos. Frente al manejo de datos personales, la Universidad y sus colaboradores (incluyendo los Teletrabajadores) deben dar cumplimiento a la legislación vigente.
- **Pública Interna:** Se clasifica así la información que se publica y tiene impacto sobre la comunidad EANista. Documentos como reglamentos internos, procedimientos, manuales y lineamientos entre otros.
- **Pública Externa:** Se clasifica así la información que pueda interesar a cualquier ente o persona interna y externa. Se publica así información como programas académicos entre otros.

LINEAMIENTOS DE SEGURIDAD PARA EL CORREO ELECTRÓNICO

Descripción

La Universidad EAN ha adoptado servicios de correo institucional, por lo tanto, se hace necesario establecer las condiciones técnicas y de seguridad sobre las cuales el estudiante, egresado, docente, colaborador, proveedor o tercero y cualquier otro que tenga un vínculo directo y así lo amerite acceda a estos recursos.

Infraestructura tecnológica

Para efectos de tener mayor cobertura y capacidades en el servicio de correo electrónico, la Universidad EAN ofrece un servicio de correo a su comunidad en:

- Correo académico y administrativo "@universidadean.edu.co": bajo este dominio se mantienen las cuentas de correo de estudiantes, docentes, egresados, colaboradores y cuentas asignadas a procesos o eventos. Este servicio se ofrece con la empresa Google en el marco del convenio de Google Apps Education.

Aspectos generales

- Cada cuenta de correo electrónico tiene asociado un conjunto de recursos de almacenamiento que es ilimitado.
- El servicio de correo administrativo permite la transferencia de archivos como adjuntos del mensaje o compartidos a través de sus herramientas.
- Las imágenes enviadas en el cuerpo del mensaje electrónico no son mayores a 10 Megabytes, un mayor peso de la imagen genera lentitud en la distribución y saturación del correo.
- Mientras no se acredite un vínculo directo, académico, laboral, o como egresado con la Universidad EAN, ninguna persona o empresa podrá solicitar cuenta de correo asociada a los dominios institucionales.
- Las cuentas de usuario de correo son generadas bajo el estándar estipulado en la creación de cuentas de la Universidad, en caso de que un usuario deba realizar un cambio de cargo se conserva la misma cuenta de correo, se parte del principio que el correo es un medio de comunicación mas no de almacenamiento de información. No obstante, el correo electrónico actualmente contratado cuenta con mecanismos propios para copias de seguridad de la información; sin embargo, se puede realizar copia de seguridad de los correos si lo desea al equipo local como medida adicional de preservación de la información, según solicitud del líder del proceso a través de la mesa de servicios definida por la Gerencia de Innovación y Desarrollo de TIC.

Administración del correo electrónico

Creación, borrado o inactivación de las cuentas de correo electrónico

- Correo administrativo "@universidadean.edu.co"

  La creación de las cuentas administrativas es realizada por el sistema de gestión de identidades.

  La inactivación de la cuenta la realizará la Gerencia de Innovación y Desarrollo de TIC, de acuerdo a la solicitud de la Gerencia de Desarrollo Humano a través del sistema de gestión de identidades una vez finalizado el contrato o por una ausencia temporal. Para realizar la inactivación de la cuenta de correo, se revisarán los siguientes aspectos:

  - Para los roles de sala general, consejo superior, rector, vicerrectores, decanos, y líderes de procesos que reportan directamente al rector, no se les inactivará la cuenta en los casos de vacaciones, permisos, incapacidades, licencias remuneradas y no remuneradas. En caso de retiro o sanción disciplinaria la cuenta debe ser deshabilitada.
  - Para los colaboradores con roles diferentes a los mencionados en el punto anterior, la cuenta de correo se inactivará para ausencias temporales (vacaciones, incapacidades, licencias remuneradas, licencias no remuneradas, permisos) mayores a cinco (5) días o en caso de sanción. Cuando se requiera apertura de la cuenta para realizar actividades especiales inherentes al rol desempeñado por el colaborador o docente, el líder del proceso debe solicitar

esta autorización a la Gerencia de Desarrollo Humano. En caso de retiro la cuenta se inactivará definitivamente.

Todo correo administrativo, en su contenido y firma debe cumplir con lo definido en el Manual de Imagen Institucional.

Ante eventos en los cuales se da por terminado un contrato, la inactivación de la cuenta procederá por un periodo de un mes, si durante este periodo no se formaliza un nuevo contrato para el colaborador se tendrá plena libertad para eliminar la cuenta de correo y toda información que esta contenga.

- Correo académico "@universidadean.edu.co"

La creación de estas cuentas corresponde a un proceso automatizado desde los sistemas de información académico y gestión de identidades. Estas cuentas son creadas según la naturaleza del usuario, así:

- *Estudiantes activos:* Con base en los criterios para creación de cuentas el sistema de información académico genera automáticamente el identificador de usuario de la cuenta de correo, esto se da solo hasta cuando el aspirante ha formalizado su matrícula, es decir al momento en que se registra el pago en el sistema. Posteriormente estará a cargo de la Gerencia de Innovación y Desarrollo de TIC, la creación de cada buzón en el servidor de correo respetando la asignación realizada por el sistema de información académico, solo así se podrá garantizar que no se dupliquen los identificadores de usuarios.

  Los estudiantes que después de dos semestres continuos no hayan matriculado unidades de estudio se consideran retirados y se inactiva la cuenta. La inactivación supone un bloqueo de la cuenta para evitar su uso. Solo con una nueva inscripción de unidades de estudio se volverá a activar la cuenta.

- *Egresados:* El egresado(a) es aquella persona que ha obtenido un título académico de pregrado o postgrado con la Universidad EAN, esta condición le permite tener una cuenta de correo vitalicia. A estas personas se les mantendrá el identificador de usuario de la cuenta de correo asignada cuando se vincularon a la Universidad. Si el egresado corresponde a promociones antiguas cuando no existía el servicio de correo electrónico, esté podrá solicitar la activación de una cuenta de correo a través de la oficina de egresados quienes a su vez formalizan la solicitud de creación de la cuenta a través del sistema de mesa de servicios de la Gerencia de Innovación y Desarrollo de TIC especificando el nombre completo y número de identificación.

- *Docentes:* Con base en los criterios para creación de cuentas el sistema de información gestión de identidades genera automáticamente el identificador de usuario de red y de la cuenta de correo, esto se da solo cuando el docente tiene contrato vigente. Posteriormente estará a cargo de la Gerencia de Innovación y Desarrollo de TIC la creación de cada buzón en el servidor de correo.
- Para el caso de los docentes de planta la cuenta de red y correo se inactivará una vez finalice su contrato.

- Para el caso de los docentes de cátedra se mantendrá la cuenta de red y de correo activa durante 75 días posteriores a la fecha de finalización del contrato, una vez finalizado este plazo, se inactivará la cuenta de red y correo.

- *Colaboradores temporales y practicantes:* Con base en los criterios para creación de cuentas, la Gerencia de Innovación y Desarrollo de TIC asignará cuentas de correo informadas únicamente por la Gerencia de Desarrollo Humano mediante el sistema de Gestión de Identidades. La cuenta estará activa hasta el momento en que finalice el contrato.

- *Cuentas de procesos y/o eventos:* Estas cuentas refieren buzones de correo creados para el intercambio de mensajería electrónica a cuentas genéricas institucionales. Para la creación de estas cuentas de correo el líder de proceso o coordinador del evento, debe hacer la solicitud justificando su creación, a través de la Secretaria General; una vez autorizada, la generación de estas cuentas estará a cargo de la Gerencia de Innovación y Desarrollo de TIC. El identificador de usuario de estas cuentas será asignado por el líder de proceso o coordinador del evento y debe tener una extensión no mayor a doce (12) caracteres.

  La vigencia de una cuenta de proceso y/o evento, estará determinada por el solicitante de la cuenta, cualquier inactivación de estas cuentas son solicitadas a través del sistema de mesa de servicio de la Gerencia de Innovación y Desarrollo de TIC. Las cuentas de proceso y/o evento que no tengan uso por un tiempo mayor a un año serán eliminadas.

- Correo Masivo

  El envío de correo masivo se realiza por medio de herramientas de mailing (masterbase, right now), listas de correo o de sistemas de información especializados en esta actividad; los cuales se constituyen en una herramienta para la comunicación con los Stakeholders, sin embargo, el uso de este recurso se realiza atendiendo los lineamientos establecidos para el uso y tratamiento de datos personales contenidos en este manual y en los manuales de procedimiento y buenas prácticas para que se tenga una comunicación efectiva sin afectar la privacidad de las personas. En este sentido la Universidad EAN dispone de listas de correo internas y sistemas de información con las cuentas correo de los colaboradores y docentes y con listas de correo externas con las cuentas de correo de estudiantes, egresados, interesados, entre otros.

  Para el uso de las listas de correo o sistemas de información de envío masivo, se han definido los siguientes lineamientos:

  Internas:

  - Las listas de correos internas solo podrán ser autorizadas por el líder del proceso solicitante y creadas por la Gerencia de Innovación y Desarrollo de TIC.
  - La lista será asignada y asociada a la dirección del correo electrónico del líder de proceso o quien responde por el debido uso y el respeto por la confidencialidad de la información enviada y protección de datos personales. Por lo tanto, se garantiza que no sea usada para el envío de correos masivos diferentes al objetivo para la cual fue creada.
  - La información que sea enviada a los grupos de correo se hace a través de copias ocultas usando CCO.

- Las listas de correo internas no están habilitadas a envíos desde cuentas de correo (dominios) diferentes a las que asigna la Universidad EAN.
- Cada usuario podrá crear sus propias listas internas o grupos de correos internos y será responsable por el debido uso, la confidencialidad de la información y la protección de los datos personales.
- Las listas de correo se limitarán a uso interno y para información institucional que requiera ser conocida por los miembros de la lista.

Listas de correo externas/Herramientas de mailing:

- Estas listas solo podrán usar la herramienta de mailing contratada por la Universidad.
- El líder de proceso podrá designar a un colaborador de su proceso como responsable de la utilización de la herramienta de mailing y en caso de indisponibilidad de la herramienta de mailing, la Gerencia de Innovación y desarrollo de TIC apoyará temporalmente, la creación de listas de correo autorizadas por la Gerencia de Innovación y Desarrollo de TIC. Los colaboradores autorizados para enviar correo masivo asumen toda responsabilidad respecto a la información que sea intercambiada con estos grupos de correo.
- Para enviar mensajes a las cuentas de correo es importante tener la aprobación del usuario (dueño de la cuenta de correo) teniendo en cuenta los lineamientos de administración de datos personales establecida por la Universidad. Es mandatorio que en los eventos o actividades de mercadeo en la que se obtiene datos de interesados se registre la autorización para recibir información a través del correo electrónico.
- Cuando un usuario informe que desea ser retirado de las listas externas o herramientas de mailing, se debe informar al correo electrónico habeasdata@universidadean.edu.co
- En caso de usar listas de correo externas, la información que sea enviada a estos grupos de correo se hace a través de copias ocultas usando CCO.

Acceso al servicio de correo electrónico

Todo usuario de la comunidad EANista que posea una cuenta de correo institucional, puede acceder a esta dentro o fuera de las instalaciones de la Universidad EAN vía web.

Uso del correo electrónico

- El correo electrónico pertenece a la Universidad EAN, bajo el contexto de uso institucional, propio de las actividades administrativas, académicos y de investigación; estando terminantemente prohibido realizar cualquier otra actividad o transacción comercial.
- El uso inapropiado del correo electrónico de la institución acarrea la aplicación de las medidas disciplinarias a que haya lugar y demás acciones legales del caso.
- Se debe evitar el envío de archivos con extensiones .EXE, .BAT, .COM, .DLL, .VBS, por razones de seguridad y para evitar propagación de virus.
- Evitar abrir correos de los cuales no se conozca el remitente y absténgase de abrir los archivos adjuntos.
- Ante la recepción de correos de carácter sospechoso, solicite la verificación del correo por la Gerencia de Innovación y Desarrollo de TIC.
- Se prohíbe usar el correo institucional para: enviar contraseñas; enviar mensajes que inciten a la comisión de delitos; reenviar archivos de los que no se conozca su origen y que no sean confiables;

distribuir información confidencial de la Universidad EAN; la difusión de insultos o información que atente contra la moral y buenas costumbres; distribuir mensajes que argumenten solicitudes de redistribución a otros correos o información publicitaria que sea diferente a los objetivos y propósitos de la Universidad EAN; enviar información que vulnere la confidencialidad de un tercero o que haga cuestionamientos públicos de la honra, la intimidad de las personas o violación de los datos personales.

- Se debe evitar usar cualquier forma engañosa de enviar correos electrónicos, como edición de fechas, remitentes, encabezados entre otros.
- Se debe evitar utilizar el correo para enviar cadenas, advertencias o cualquier tipo de mensaje similar.
- Se debe evitar usar claves de acceso débiles o fáciles de adivinar tales como: nombre propio, la palabra universidad, la palabra escuela, nombre de algún familiar cercano, fechas de nacimiento, aniversario, nombre de mascota, número de identificación, entre otras.
- Se recomienda cambiar la clave del correo, cuando ingrese por primera vez y de forma periódica.
- Toda la información contenida en los buzones de correo institucionales es propiedad de la Universidad EAN por lo tanto puede ser inspeccionada en cualquier momento a solicitud de los organismos de control interno o por requerimientos judiciales sin previo consentimiento del usuario de la cuenta de correo.
- Ninguna persona está autorizada para acceder a información de otro usuario. Solamente por motivos jurídicos o disciplinarios se abrirán los archivos a las instancias correspondientes, previo permiso de una autoridad competente.
- La Gerencia de Innovación y Desarrollo de TIC es responsable de tomar las medidas necesarias para que el servidor no admita adjuntos en el correo que tengan virus informáticos, no obstante, se mantiene actualizado el sistema de antivirus de los equipos de cómputo propiedad o a cargo de la Universidad.
- Los equipos propiedad o a cargo de la Universidad cuentan con actualización del antivirus periódica, no se autoriza la desinstalación del mismo, la instalación de otra versión o marca del software de antivirus.
- La Gerencia de Innovación y Desarrollo de TIC podrá implementar las acciones que limiten el uso de las listas de correo, los correos masivos y los grupos de correo o cualquier otra denominación que vulnere la confidencialidad de la información personal o ponga a la Universidad en listas negras ante las autoridades de internet o en otras instituciones.
- En caso de detectarse remitentes internos que estén haciendo distribución de mensajes inapropiados son notificados a la Gerencia de Innovación y Desarrollo de TIC, para proceder al bloqueo o la inactivación de la cuenta e informar a las respectivas instancias para la aplicación de las medidas disciplinarias que estén contempladas en el reglamento interno de trabajo o el reglamento estudiantil.
- En caso de detectarse remitentes externos que estén haciendo distribución de mensajes inapropiados son notificados a la Gerencia de Innovación y Desarrollo de TIC para proceder al bloqueo en los sistemas de seguridad de la Universidad.
- El usuario dueño del buzón es responsable de todos los mensajes de correo que sean enviados a su nombre.
- Se informa a la Gerencia de Innovación y Desarrollo de TIC sobre cualquier anomalía que sea detectada en el correo, así como la apertura de un correo sospechoso o cualquier alerta generada por el antivirus o en caso de detectar algún tipo de incidente de seguridad.
- En caso de que se use, la cuenta de correo como colaborador y estudiante o docente y estudiante, al finalizar el contrato de colaborador o docente se inactivará la cuenta de correo y se creará una nueva, teniendo en cuenta las condiciones para estudiante.

- En caso de que se use, la cuenta de correo como colaborador y egresado o docente y egresado, al finalizar el contrato de colaborador o docente se inactivará la cuenta de correo y se creará una nueva, teniendo en cuenta las condiciones para egresado.
- Cuando se retira un colaborador o docente y se inactiva la cuenta de correo, se podrá establecer un mensaje de respuesta con el nuevo contacto a solicitud del líder del proceso. También se podrá trasladar la información de la cuenta inactiva a otro buzón, para evitar el uso de la cuenta de correo inactiva.

Son considerados actos inapropiados contra el servicio de correo electrónico en la Universidad EAN aquellos que afecten la disponibilidad del servicio tales como:

- Ataques de denegación de servicios a los servidores de la Universidad EAN o que a través de la universidad se realicen hacia terceros.
- Ataques de fuerza bruta para obtener credenciales de acceso a cualquier servidor o servicio de la Universidad EAN o utilizar la infraestructura de la Universidad para realizar cualquier ataque hacia terceros.
- Envío de correo masivo sin las autorizaciones correspondientes desde el correo de la Universidad EAN.
- Envío de información pornográfica u otra información que estimule la comisión de delitos.
- Accesos no autorizados a sistemas de correo de la Universidad EAN.
- Intercambio de mensajes que vaya en contra de la ley de derechos de autor o desfavorezca la protección de la propiedad intelectual o datos personales.
- Cualquier acto contrario a las presentes condiciones de uso será considerado un acto inapropiado y será sancionado conforme a las normas internas vigentes y a la legislación colombiana si el acto lo amerita.

LINEAMIENTOS DE SEGURIDAD PARA EL USO DE MEDIOS DE ALMACENAMIENTO EXTRAÍBLES O REMOVIBLES

Descripción

La utilización de dispositivos removibles o extraíbles de almacenamiento (Memorias USB/Flash, SD, microSD, CD/DVDs re escribibles, discos duros portátiles, dispositivos electrónicos como celulares, tablets, entre otros) por parte de los usuarios, se encuentra restringido y monitoreado, y podrá ser autorizado a algunos colaboradores directos de la Universidad EAN que lo requieran, cumpliendo con los lineamientos estrictamente establecidos por la Universidad. El colaborador que los utilice con la autorización respectiva deberá buscar en todo momento preservar la Confidencialidad de la información de la Universidad EAN almacenada en éste, así como evitar contagiar la red de la Universidad de código malicioso o dañino (virus, troyanos, Spyware, etc.).

Uso de medios de almacenamiento extraíbles

- Evitar hacer copias de respaldo de información en estos medios, se debe guardar en los repositorios institucionales para el almacenamiento de información, según corresponda.
- No se divulga, ni transfiere la información almacenada en los medios extraíbles a personas ajenas a la institución. Esto puede comprometer la confidencialidad de la información de la Universidad.
- Los usuarios o personas que pertenezcan a servicios tercerizados contratados por la Universidad, no podrán utilizar dispositivos removibles o extraíbles de almacenamiento (Memorias USB/Flash, SD,

microSD, CD/DVDs re escribibles, discos duros portátiles, dispositivos electrónicos como celulares, tablets, entre otros) diferentes a los asignados y autorizados para cumplir o ejecutar sus labores en las instalaciones teniendo en cuenta situaciones en las cuales posea o manipule información de la Universidad.

- El servicio de navegación prestado por la Universidad EAN es suministrado y autorizado únicamente para propósitos del negocio, y podrá ser restringida o limitada a áreas consideradas confidenciales, debido a que gestionan o manipulan información clasificada como confidencial o sensible para la Universidad.

Si se utiliza los medios de almacenamiento extraíbles autorizados en un equipo de cómputo diferente al de la Universidad se tiene en cuenta las siguientes recomendaciones:

- Copiar información almacenada en los medios de almacenamiento extraíbles a los discos locales del equipo de cómputo asignado solamente después del escaneo previo.
- Al momento de conectar los medios de almacenamiento extraíbles al equipo de cómputo de la Universidad EAN, realiza un escaneo previo con el antivirus autorizado por la Institución, con el fin de evitar que se transfieran virus informáticos y software malicioso.
- No exponer los medios de almacenamiento extraíbles en lugares públicos.
- Proteger los medios de almacenamiento extraíbles de humedad y golpes.
- Evitar consumir bebidas durante la utilización de los medios extraíbles.

LINEAMIENTOS DE SEGURIDAD PARA COPIAS DE RESPALDO

Descripción

Los sistemas de información que almacenan, procesan o transmiten información clasificada como confidencial, en infraestructura tecnológica propia de la Universidad (Físicos o virtuales) o contratados a terceras partes (Físicos o en Internet), deberán asegurar la generación de copias de respaldo, su periodo de retención, rotación y métodos apropiados para su restauración. Estas copias de seguridad deben estar en lugares apropiados cumpliendo los requisitos de condiciones ambientales y de seguridad, en custodia para garantizar su integridad y disponibilidad y realizar una verificación periódica que los datos retenidos en los medios son fiables y garantizan una recuperación de los sistemas.

Las copias de respaldo de todos los sistemas de información y/o aplicativos contenidos en los servidores de la Universidad EAN se realizan bajo los lineamientos establecidos en el documento TIC-301 Generación y Restauración de Copias Respaldo que se encuentre vigente, bajo la responsabilidad de la Gerencia de Innovación y Desarrollo de TIC.

Desde la Gerencia de Innovación y Desarrollo de TIC no se realizan copias de respaldo de los equipos de cómputo de los colaboradores, dado que la información relevante e importante para el rol del colaborador se debe almacenar en los repositorios asignados como los son los gestores de carpetas, google drive y gestión documental, herramientas de apoyo y almacenamiento de archivos electrónicos.

En casos especiales que se necesite realizar copia de respaldo de un equipo específico, la solicitud se debe realizar a la Gerencia de Desarrollo Humano, quien comunicará a la Gerencia de Innovación y Desarrollo de TIC.

Restauración de copias de respaldo

Mediante el proceso de restauración de copias de respaldo se logra obtener información que por causas diversas sufrió pérdida o modificación, se requiera verificar datos que por alguna razón no son consistentes o para realizar pruebas de integridad. Dicha restauración se realiza bajo los lineamientos establecidos en el documento TIC-301 Generación y Restauración de Copias Respaldo que se encuentre vigente.

Respaldo de servicios alojados en internet o en sitios alternos de proveedores de servicios

- *Para servicios en modalidad de Colocación:*
  - Bajo este modelo la responsabilidad de la realización de las copias de respaldo recae en la Universidad EAN, por lo cual deberá realizarse bajo los lineamientos establecidos en el documento TIC-301 Generación y Restauración de Copias Respaldo que se encuentre vigente.
  - Se realizan copias de respaldo de aplicaciones y datos según la evaluación de las necesidades asociadas a cada uno de los servicios.

- *Para servicios en modalidad de Alojamiento Web:*
  - Cuando se contrate o configure un servicio en la modalidad de hosting, a través del contrato el proveedor debe garantizar la realización de copias de respaldo periódicos a los datos, las aplicaciones y demás información según las necesidades de cada servicio.
  - Las copias de respaldo realizadas son entregadas de forma periódica al líder técnico de la aplicación de la Universidad EAN, ya sea en medios magnéticos o mediante el acceso a un repositorio.
  - Si las copias de respaldo se entregan en medios magnéticos, estos se revisan y se envían debidamente etiquetados con el proveedor del servicio de custodia que tiene contratado la Universidad.
  - El proveedor garantiza contractualmente la confidencialidad de la información que se encuentre alojada en sus equipos, teniendo en cuenta los lineamientos definidos en este manual para la administración de datos personales y un contrato de transmisión de datos vigente.
  - Se tiene en cuenta las tablas de retención de información para las copias de respaldo de acuerdo a lo definido en la Universidad.
  - Al finalizar el contrato, el proveedor debe entregar copia de toda la información de la Universidad en un formato estándar y legible.

- Para servicios en Cloud (IaaS, PaaS, SaaS):
  - Cuando se contrate o configure un servicio con información en la nube (Cloud) bajo cualquiera de las modalidades de Infraestructura como servicio, Plataforma como servicio o Servicio como servicio, a través del contrato el proveedor debe garantizar la realización de copias de respaldo periódicas a los datos acordados según la evaluación de necesidades (información en archivos o estructurada, aplicaciones, sistemas operativos o cualquier otro tipo de información aplicable).
  - Los tipos de copias de seguridad (completo, incremental, diferencial o réplica en línea) y su periodicidad es definida por la Universidad EAN y el proveedor contractualmente según las necesidades del servicio contratado.

- Las copias de respaldo realizadas son entregadas de forma periódica al líder técnico de la aplicación de la Universidad EAN, ya sea en medios magnéticos o mediante acceso a un repositorio.
- Si las copias de respaldo se entregan en medios magnéticos, estos se envían debidamente etiquetados con el proveedor del servicio de custodia que tiene contratado la Universidad.
- El proveedor garantiza contractualmente la confidencialidad de la información que se encuentre alojada en sus equipos, teniendo en cuenta los lineamientos definidos en este manual para la administración de datos personales y un contrato de transmisión de datos vigente.
- Se tiene en cuenta las tablas de retención de información para las copias de respaldo de acuerdo a lo definido en la Universidad.
- Al finalizar el contrato, el proveedor debe entregar copia de toda la información de la Universidad en un formato estándar y legible.

LINEAMIENTOS DE SEGURIDAD PARA LOS REPOSITORIOS INSTITUCIONALES

Descripción

La Universidad EAN ofrece tres tipos de repositorios institucionales, con el propósito de garantizar el respaldo y asegurar, proteger y centralizar la información de cada proceso. El acceso a los repositorios institucionales se da a través del usuario y contraseña asignados a los colaboradores para la sesión de red o cuenta de correo electrónico; por lo cual el acceso a los repositorios es responsabilidad exclusiva de los colaboradores.

La Gerencia de Innovación y Desarrollo de TIC, garantiza la disponibilidad de los repositorios institucionales.

Uso de los repositorios institucionales

- Evitar divulgar y/o transferir la información sensible almacenada en los repositorios institucionales a personas no autorizadas.
- El usuario al cual se asigna un equipo de cómputo, es el único responsable del equipo asignado y de la información de la Universidad a la que se acceda a través de este.
- Las credenciales asignadas para el acceso a los repositorios institucionales son de uso personal e intransferible.
- El usuario es responsable de bloquear la sesión de red o su cerrar su cuenta de correo electrónico al momento de levantarse del puesto de trabajo.
- La información almacenada en los repositorios institucionales por parte de los procesos debe cumplir con lo establecido en el reglamento de propiedad intelectual resolución 144 del 20 de noviembre de 2013 o en su defecto el que se encuentre vigente.

A. La información que se guarda en estos repositorios institucionales es la siguiente:

- Información relacionada en el listado maestro de registros del sistema de gestión de calidad, que incluye las tablas de retención documental.
- Información que este en versión final (Informes, presentaciones, planos, hojas trabajo, actas de reunión, entre otros)
- Información que cada proceso considere importante para el desarrollo de sus actividades y/o que deba mantenerse bajo controles de seguridad y con su respectivo respaldo y protección, para mitigar el riesgo de pérdida de información o acceso indebido o no autorizado a la misma.

- La información activa en los repositorios institucionales tiene una vigencia de un (1) año. Información con mayor antigüedad será guardada a nivel de históricos a los cuales se tendrá acceso únicamente con permisos de lectura.

B. La información que NO se guarda en las unidades de red o carpetas compartidas es la siguiente:

- Información personal, música en cualquier formato, videos, fotos e imágenes cuya propiedad intelectual no sea de la Universidad o que vaya en contra de las normas vigentes relacionadas con derechos de autor y privacidad.
- Información cuya procedencia sea desconocida.
- Información que no se considere relevante para la normal ejecución de las actividades de cada proceso debe guardarse en los discos locales (Unidades nombradas con C y/o D) del equipo de cómputo asignado a cada usuario.

C. Para el almacenamiento y asignación de nombres a los archivos que se guarden en los repositorios institucionales (carpetas compartidas) se tiene en cuenta:

- La estructura de carpetas de los repositorios asignados a cada proceso ha sido definida de acuerdo a lo siguiente:
  -> Carpeta con Nombre de proceso
  -> Subcarpeta del año
  -> Subcarpetas por áreas o subprocesos
  -> Subcarpeta compartida para el proceso

  Para cualquier información almacenada fuera de esta estructura no será realizada copia de respaldo.

- Los permisos a los repositorios institucionales de cada proceso son asignados a los colaboradores que pertenecen al respectivo proceso. Se asignan permisos de escritura sobre las carpetas propias y permisos de lectura sobre las otras carpetas del proceso. Para la carpeta compartida del proceso se asignan permisos de escritura y lectura para todos los colaboradores del proceso.
- Los nombres de las carpetas y archivos contienen máximo 32 caracteres de esta forma se garantiza que la copia de respaldo se haga correctamente.
- Los nombres de las carpetas y archivos no deben tener caracteres especiales como: ñ, tilde, _, %,*, /, entre otros).
- Los nombres de las carpetas y archivos no deben tener nombres propios de colaboradores o contar con nombre por defecto (Nueva carpeta).
- Atender las especificaciones respecto a la clasificación que desde gestión documental se defina para la asignación de nombres de archivo.
- Cada proceso contará con un responsable de la gestión del repositorio institucional asignado al proceso quien se encargará de velar por el adecuado manejo y conservación de la estructura de almacenamiento definida en este lineamiento.
- Archivos con información sensible o confidencial deben contar con contraseña para proteger su confidencialidad.

Para solicitar la recuperación de información de la copia respaldo de los repositorios institucionales se realiza la solicitud a la Gerencia de Innovación y Desarrollo de TIC a través de la mesa de servicio y la atención de

estos requerimientos se hará conforme al procedimiento definido en el sistema de gestión de calidad, documento TIC-301 Generación y Restauración de Copias Respaldo que se encuentre vigente.

LINEAMIENTOS DE SEGURIDAD PARA LA ADMINISTRACIÓN DE CUENTAS Y CONTRASEÑAS DE USUARIO

Descripción

El acceso a la mayoría de los servicios de tecnología se da por medio de la validación de un nombre de usuario y una contraseña, por lo tanto, es necesario definir los lineamientos para que estas credenciales de acceso tengan los elementos de seguridad básicos para minimizar el riesgo de acceso por parte de personas no autorizadas.

Administración de cuentas

La administración de cuentas contempla los distintos tipos de cuenta y las medidas pertinentes para la vinculación o la desvinculación del personal directo o de terceros en la Universidad. Entre ellos se crea, cancela o deshabilita los permisos de acceso a los sistemas de información de la Universidad que el usuario utilice y se elimina cualquier vínculo a nivel de publicaciones y de cualquier tipo contractual que se encuentre habilitado.

Cuentas normales

- La Gerencia de Desarrollo Humano a través del sistema de Información Gestión de Identidades, informará a la Gerencia de Innovación y Desarrollo de TIC y a cada líder funcional de los sistemas de información y/o aplicativos la cuenta para cada colaborador o docente, a su vez, estos se encargarán de asignar las cuentas, con los perfiles correspondientes a cada sistema de información para desempeñar el cargo.
- Las cuentas de usuario para estudiantes se asignan una vez el sistema de información académico, genere automáticamente el identificador de usuario, es decir, cuando el aspirante haya formalizado su matrícula.
- Las cuentas de usuario serán la identificación única para acceder a los diferentes sistemas de información y/o aplicativos y recursos informáticos de la Universidad.
- Cada cuenta de usuario normal tiene los privilegios de accesos debidamente autorizados para desempeñar las labores propias al cargo para el cual fue contratado.
- La Gerencia de Desarrollo Humano reporta a la Gerencia de Innovación y Desarrollo de TIC y a los líderes funcionales, las novedades mayores a cinco días para deshabilitar las cuentas de usuario de manera temporal o definitiva, según sea el caso.
- Las cuentas de los docentes y colaboradores son generadas a través de la herramienta gestión de identidades.
- La inactivación de la cuenta, la realiza la Gerencia de Desarrollo Humano a través del sistema de gestión de identidades una vez finalizado el contrato o por una ausencia temporal. Para realizar la inactivación de la cuenta, se revisarán los siguientes aspectos:

    - Para los roles de sala general, consejo superior, rector, vicerrectores, decanos, y líderes de procesos que reportan directamente al rector, no se les inactivará la cuenta en los casos de vacaciones, permisos, incapacidades, licencias remuneradas y no remuneradas. En caso de retiro o sanción disciplinaria la cuenta debe ser deshabilitada.

- Para los colaboradores con roles diferentes a los mencionados en el punto anterior, la cuenta se inactivará para ausencias temporales (vacaciones, incapacidades, licencias remuneradas, licencias no remuneradas, permisos) mayores a cinco (5) días o en caso de sanción. Cuando se requiera apertura de la cuenta para realizar actividades especiales inherentes al rol desempeñado por el colaborador o docente, el líder del proceso debe solicitar esta autorización a la Gerencia de Desarrollo Humano. En caso de retiro la cuenta se inactivará definitivamente.

Cuentas privilegiadas

Se entiende como cuentas privilegiadas aquellas credenciales de acceso con privilegios de administración sobre los sistemas de información, motores de bases de datos o software base (sistemas operativos). Estas cuentas son asignadas normalmente a los técnicos de la Gerencia de Innovación y Desarrollo de Tecnologías de Información y Comunicación y por sus privilegios sobre los sistemas, los rigen los siguientes lineamientos.

- La Gerencia de Innovación y Desarrollo de TIC, define uno o varios responsables para la administración de cuentas de usuarios técnicos y cuentas de usuarios funcionales de los recursos informáticos. Los usuarios técnicos y funcionales tienen una identificación única de usuario.
- Se habilita log de registro cuando se requiera, con el fin de tener trazabilidad de los usuarios privilegiados, en caso de alguna falla o denegación de algún servicio.
- Se retira o bloquea los accesos de las cuentas de usuario que han cambiado de función, o que se han retirado de la institución.
- Usar las cuentas de administración privilegiadas de administración para instalación, actualización, modificación de programas, o modificaciones a las bases de datos.
- En caso de ser necesario el uso de las cuentas de usuario de administración; la Gerencia de Innovación y desarrollo de TIC es responsable de asignar dos personas autorizadas por cada sistema para el manejo, custodia de dichas cuentas, y documentar la razón por la cual se utiliza.
- Cualquier actividad que involucre modificación directa de una fuente de datos (bases de datos) de sistemas de información productivos, mediante cuentas privilegiadas debe ser solicitada por el líder funcional y aprobada por el líder de proceso respectivo y La Gerencia de Innovación y Desarrollo de TIC. Solo aplica para solicitudes que no se pueden realizar por el sistema de información.

Cuentas de procesos

Corresponden a las cuentas que se asignan para que un grupo de colaboradores accedan a Sistemas de Información y/o Aplicaciones, empleando un único usuario y contraseña.

- El uso de las cuentas de usuario de procesos, son aprobadas por la Gerencia de Innovación y Desarrollo de TIC y el líder funcional del sistema de información.
- Se define su función y se realiza la respectiva documentación que describa el uso y los privilegios asignados a la cuenta.
- Se habilita log de registro de las cuentas de usuarios de procesos con el fin de tener trazabilidad de las modificaciones que realice.
- Realizar depuración y bloqueo o eliminación de las cuentas de usuarios de procesos en el momento que no se requiera su uso.

Cuentas de proveedores que prestan servicios de tecnología

- La Gerencia de Innovación y desarrollo de TIC asigna a cada proveedor un usuario y contraseña propia únicamente cuando sea necesario para el desarrollo de los servicios contratados y con los privilegios correspondientes.
- La Gerencia de Innovación y desarrollo de TIC evita que el proveedor haga uso de las cuentas de administración, para los mantenimientos, actualizaciones, migraciones que realicen en los recursos informáticos y sistemas de información.
- En caso de ser necesario la utilización de las cuentas de administración, no se divulgan las credenciales de acceso. La persona encargada de custodiar dichas credenciales de acceso las digita cuantas veces el proveedor lo requiera.
- La contraseña tiene mecanismos de cifrado.
- El líder técnico realiza monitoreo continuo a la labor que esté realizando el proveedor.
- Se habilitar log de registro de las cuentas de usuario de proveedores.
- En el momento que el proveedor ya no requiera el uso de la cuenta esta se desactiva.

Administración de contraseñas

Para cuentas normales y proveedores que prestan servicios de tecnología

Las mismas descritas en los numerales 2.6.2.1 y 2.6.2.4

Para cuentas privilegiadas

- Las contraseñas predeterminadas por el proveedor se cambian inmediatamente después de la instalación de los recursos informáticos, sistemas información o del software.
- Las contraseñas de usuarios de administración se cambian al menos dos veces al año y cuentan con mecanismos de cifrado.
- Se definen dos personas responsables de custodiar las contraseñas de las cuentas de usuarios privilegiados.

Uso de cuentas y contraseñas de usuario

- Todas las credenciales asignadas son de uso personal e intransferible, por tanto, no se comparten ni divulgan bajo ninguna circunstancia.
- Evitar usar contraseñas de acceso débiles o fáciles de adivinar como: nombre propio, la palabra universidad, la palabra escuela, nombre de algún familiar cercano, fechas de nacimiento, aniversario, nombre de mascota, número de identificación, entre otras.
- Evitar almacenar las contraseñas en sistemas de computador, en archivos de software o dispositivos, manuales o formatos no protegidos.
- Evitar dejar las contraseñas en un lugar visible a personas no autorizadas.
- Evitar formar contraseñas con números y/o letras que estén adyacentes en el teclado. Ejemplos: 123456, 1q2w3e o 123QWEasd.
- Evitar el uso de contraseñas grupales, compartidas o genéricas.
- Las contraseñas contienen una longitud mínima de 8 caracteres.
- Son alfanuméricas, es decir contiene números, letras y caracteres especiales.

- Evitar la reutilización de contraseñas antiguas por lo menos de doce meses atrás.
- Cambiar la contraseña periódicamente cada tres meses.

Desvinculación o cambio de rol de colaboradores y terceros

La desvinculación o cambio de rol contempla los distintos tipos de cuenta y las medidas pertinentes para la desvinculación del personal directo o de terceros de la Institución. Se informa de manera oportuna las novedades de desvinculación o cambio de rol a los líderes de proceso para que ellos se encarguen de garantizar el cumplimiento de las actividades tecnológicas pertinentes para estos casos realizando el reporte a la Gerencia de Innovación y desarrollo TIC y a los líderes funcionales que administran aplicaciones. Estas actividades incluyen:

- Validar la entrega formal de la información propia de su cargo, esta incluye la entrega de calificaciones para el caso de docentes.
- Realizar copias de respaldo de la información institucional que el líder de proceso considere pertinente en los repositorios compartidos de cada proceso teniendo en cuenta los listados maestros de calidad.
- La Gerencia de Desarrollo Humano reporta la desvinculación laboral para que la Gerencia de Innovación y Desarrollo de TIC elimine o deshabilite los accesos remotos (VPN), elimine o inactive los accesos asociados al correo institucional.
- La Gerencia de Desarrollo Humano reporta la desvinculación laboral para que los líderes funcionales que administran sistemas de información de la universidad EAN eliminen o bloqueen los accesos.
- Los cambios de rol a nivel interno se reflejan en el retiro de todos los derechos de acceso que no sean aprobados para el nuevo rol.
- Retirar o adaptar derechos de acceso, incluyendo acceso físico y lógico, llaves, tarjetas de identificación, subscripciones y retiro de cualquier documentación que los identifica como un miembro actual de la universidad.
- Si un colaborador, contratista o usuario de tercero desvinculado tiene conocimiento de contraseñas de usuario de cuentas administradoras, deben ser modificadas para garantizar la confidencialidad y disponibilidad de la información.
- Informar a los editores y web master de la universidad para que se elimine o adapte el contenido de artículos y/o publicaciones donde se haga referencia al colaborador o tercero desvinculado.
- Garantizar la entrega de contraseñas por parte de los líderes funcionales y la respectiva documentación frente al sistema de información.

LINEAMIENTOS DE SEGURIDAD PARA LA CLASIFICACIÓN, RECICLAJE Y/O DESTRUCCIÓN DE LA INFORMACIÓN

Descripción

La información en la Universidad EAN para efectos del manejo se clasifica en: información sensible o confidencial e información pública.

El ciclo de vida de la información consta de tres etapas: generación, conservación y destrucción, por tanto, cada etapa contiene un procedimiento para garantizar su buen uso y confidencialidad. (Ver Manual FRF-313 Gestión Documental, en el Sistema de Información – ISOLución®)

Información sensible o confidencial

Es considerada como aquella información privada o confidencial que al ser divulgada puede causar algún daño o perjuicio a la institución y a sus Stakeholders, por lo tanto, requiere de un manejo adecuado y seguro. Esta información se clasifica en:

- Datos personales de los estudiantes e información en hoja de vida.
- Notas académicas.
- Datos personales de los colaboradores e información relevante en hoja de vida. (Ley 1266 de protección de datos)
- Datos personales de los docentes de planta y de cátedra.
- Información financiera.
- Procesos de investigación.
- Listados maestros de calidad.
- Registros de consultas médicas del servicio médico.
- Registros de consultas de Consejería Estudiantil.
- Registros de campañas de mercadeo.
- Listas de contactos de la Vicerrectoría de Extensión y Proyección Social.
- Encuestas y estudios de factibilidad para la creación de programas.
- Registros de nómina.
- Producción Intelectual de la Universidad.
- Diagramas de red de la Universidad.
- Información académica de los egresados que este bajo la administración de la universidad.
- Información sobre la gestión de rectoría
- Información valiosa sobre las estrategias, para el desarrollo y crecimiento de la universidad.
- Información de proyectos.
- Documentos de Planeación y Diseño de Programas.
- Procesos Legales.
- Seguimiento al Plan de Acción.
- Actas y acuerdos del Consejo Superior
- Soportes de las actas y acuerdos del Consejo Superior

Información pública

Es todo registro, archivo o dato que se recopile, mantenga, procese o se encuentre en poder de entidades públicas y/o privadas, que sea de acceso libre. No tiene el carácter sensible o confidencial.

Administración de la información sensible o confidencial

Para un manejo adecuado y custodia de la información sensible o confidencial almacenada en cualquier medio como: sistemas de información, repositorios institucionales, dispositivos de almacenamiento local, medios extraíbles, correo electrónico, medio físico, se tiene en cuenta las siguientes recomendaciones:

- La información sensible o confidencial de la Universidad almacenada en cualquier medio (físico, digital, USB, CD, otros), no se divulga a personas no autorizadas.
- El área o usuario responsable de la información es quien define quienes tienen autorización para acceder, hacer uso, o transferir la información catalogada como sensible o confidencial.
- La información sensible o confidencial se guarda en los repositorios institucionales que asigna la Gerencia de Innovación y Desarrollo de TIC, las cuales tendrán mecanismos de control de acceso para que solo las personas autorizadas puedan acceder. (Ver 2.5 Lineamientos de Seguridad para los Repositorios Institucionales)
- La Información sensible o confidencial, así como los medios de almacenamiento que la contienen es identificada. Se recomienda colocar para el caso de los documentos físicos o digitales como pie de página la frase "Información sensible o confidencial. Para uso exclusivo del personal autorizado de la Universidad EAN", sin que este altere la lectura del documento.
- Para medios de almacenamiento tales como: carpetas físicas, medios ópticos y magnéticos, se recomienda utilizar una etiqueta o rótulo con la misma frase.
- Para la información sensible o confidencial que este en medio físico el colaborador asignado por el área y el líder son responsables por la custodia y preservación de la misma; se recomienda no dejarla expuesta, guardarla en un lugar seguro.
- Bloquear manualmente el equipo de cómputo ante ausencia del colaborador de su equipo de trabajo, presionando las teclas Ctrl+Alt+Supr, opción bloquear el equipo o las teclas del símbolo de Windows + L, para evitar que la información sensible o confidencial sea expuesta.

Administración del respaldo de la información

- El líder de cada proceso define el tiempo de retención de la información digital, para asegurar que se le realice la debida copia de respaldo asociado a listado maestro de registros calidad.
- Únicamente se realiza copia de respaldo, a la información almacena en los repositorios institucionales asignado a cada proceso.
- Se tiene un sistema actualizado de copias de respaldo de la información de los diferentes procesos, para poder reinstalar fácilmente en caso de sufrir un incidente se seguridad que afecte la disponibilidad e integridad de los datos.
- Se determina el medio y las herramientas a utilizar para la generación de copias de respaldo bajo la responsabilidad de la Gerencia de Innovación y Desarrollo de TIC.
- Se define el método empleado para realizar la copia de respaldo (completo, incremental, o diferencial), de acuerdo a la criticidad y el tipo de información, según la definición de cada área o responsable de la información con el apoyo de la Gerencia de Innovación y Desarrollo de TIC.
- Se tiene un procedimiento para verificar la integridad de las copias de respaldo, que incluye una bitácora diaria que contiene la información de los que se realizaron, los que presentaron fallas y las acciones realizadas.

Uso de la información (Clasificación, Reciclaje y/o Destrucción de la información)

- Las credenciales asignadas para el acceso a la información sensible son de uso personal e intransferible, por tanto, no se comparte ni divulga.
- No deje las contraseñas en un lugar visible a personas no autorizadas.

- No genere claves fáciles de adivinar como: nombre propio, la palabra universidad, la palabra escuela, nombre de algún familiar cercano, fechas de nacimiento, aniversario, nombre de mascota, número de identificación, entre otras.
- No almacene las contraseñas en sistemas de computador, en archivos de software o dispositivos, manuales o formatos no protegidos.
- Cada área o responsable de la información define el tiempo de retención y vida útil de la información, según (TRDS) Tablas de Retención Documental y Listado Maestro de Registros del Sistema de Gestión de Calidad.
- Todos los procesos de destrucción de información cumplen con la ley de protección de datos, y asegurar que ningún tipo de información sensible o confidencial caiga en manos inapropiadas. La información que ha sido catalogada como información sensible o confidencial es reciclada solo cuando ya no sea necesaria o cuando haya cumplido su ciclo de vida útil y esté debidamente destruida. Esto evitaría que la información sea reconstruida y recuperada por de personas no autorizadas.
- A partir de la definición del tiempo de retención de la información, se realiza la copia de respaldo y así mismo se define el proceso para la destrucción del medio magnético, cuando la información cumpla su vida útil.
- Se aplican las leyes vigentes colombianas que tengan impacto en la seguridad de la información.

LINEAMIENTOS DE SEGURIDAD PARA LA GESTIÓN DE INCIDENTES

Descripción

Para la Universidad EAN, un *Incidente de seguridad de la información* es un evento o serie de eventos de seguridad que atentan contra la *Confidencialidad, y/o Integridad y/o Disponibilidad* de la información y de los recursos tecnológicos que la soportan, y que tiene(n) una probabilidad significativa de comprometer las operaciones de la Universidad y amenazar la seguridad de la información.

Tipos de incidentes

Violación de una política de seguridad: Violación de las políticas de Seguridad de la información de la Universidad EAN, incluidas en el Manual de Seguridad de la Información; comprometiendo información de propiedad de la Universidad.

Robo o pérdida de dispositivos o recursos de Hardware: Pérdida física de un recurso tecnológico (computadores de escritorio, portátiles, celulares, servidores, equipos de telecomunicaciones) de propiedad de la Universidad EAN o compromiso del mismo, por pérdida de su configuración.

Instalación de Software no autorizado: Un colaborador, tercero de la Universidad EAN o persona no autorizada, instala software en los recursos o componentes tecnológicos de la Universidad (servidores o equipos de cómputo) sin permiso o autorización de la Universidad.

Denegación de Servicio: Tipo de ataque específico que impide o dificulta el uso normal de información o recursos de la Universidad como redes de comunicaciones, sistemas de información (Sistema académico, Sistema financiero, etc.) y/o componentes tecnológicos (servidores, equipos de telecomunicaciones, portales web como universidadean.edu.co), por agotamiento excesivo de sus recursos (memoria, procesador, almacenamiento, etc.).

Actividad de virus informáticos: Un virus, gusano, troyano, botnets, keylogger, rootkit, apt, código malicioso etc., que se base en código desarrollado con el propósito de infectar una estación de trabajo, servidor o sistemas de la Universidad EAN, con el fin de capturar contraseñas o información confidencial, modificar registros de auditoría, para esconder o eliminar actividades no autorizadas.

Un virus que crea una puerta trasera debe ser manejado como un incidente de virus informático no como un incidente de acceso no autorizado.

Acceso no autorizado: Una persona obtiene acceso (intencional o inadvertido) lógico o físico sin permiso o autorización a una red o recurso de la Universidad, sistemas de información o aplicaciones (Sistema académico, sistema de nómina y recurso humano, sistema financiero, etc.), información (p.e. información de logs, bases de datos, datos personales de estudiantes de la Universidad) y en general cualquier recurso tecnológico bajo la custodia de la Universidad EAN.

En este caso también es contemplada la situación en la que un acceso no autorizado, deriva en divulgación de información clasificada como confidencial, sensible o de uso interno de La Universidad EAN o de sus estudiantes o clientes.

Divulgación o fuga de información: Este incidente consiste en la pérdida o revelación de información catalogada como sensible o confidencial de forma intencional o no intencional, a través de impresoras, equipos de cómputo, correo, internet y red, entre otros.

Actividad de Reconocimiento (escaneo de puertos y vulnerabilidades, intento de acceso, monitoreo no autorizado): Cualquier actividad que busca acceder o identificar estaciones de trabajo, puertos, protocolos, servicios en servidores o cualquier recurso de IT, o cualquier combinación para después explotar. Esta actividad no resulta en un compromiso o ataque de denegación de Servicio.

Reporte gestión de incidentes

- Todos los colaboradores, docentes, estudiantes y proveedores externos son responsables por reportar en forma inmediata y mediante los canales y medios destinados (mesa de servicio) para tal fin, cualquier condición anormal o vulnerabilidad que detecten en el uso de los recursos informáticos y/o de la información de la Universidad EAN, así como la violación de los lineamientos de Seguridad de Información de la Universidad por parte de colaboradores, estudiantes o terceros.

Gestión de incidentes

- La administración de los incidentes de Seguridad de la Información estará a cargo de la Gerencia de Innovación y Desarrollo de TIC de la Vicerrectoría Financiera de la Universidad.
- Todo incidente o alerta de seguridad debe ser tratado de principio a fin mediante un procedimiento de tratamiento de incidentes que garantice el análisis, investigación, documentación, solución, seguimiento a los mismos y en algunos casos permita adelantar acciones administrativas/legales correspondientes.
- La *Gerencia de Innovación y Desarrollo de TIC* es la responsable de analizar y determinar qué eventos son considerados incidentes de Seguridad de la Información, así como de realizar la categorización y priorización de los mismos.

- La Universidad EAN o el área que ésta defina es la responsable de definir e implementar un *Equipo de respuesta a incidentes (en adelante GRI)* con las habilidades, experiencia y recursos adecuados para la gestión y respuesta ante incidentes de seguridad de la información.
- El Grupo de Respuesta a Incidentes, debe analizar y validar cada incidente reportado y determinar el alcance de los incidentes, tal como redes, sistemas o aplicaciones afectadas, origen del incidente de seguridad reportado, herramientas o métodos de ataque utilizados, vulnerabilidades explotadas y daños causados por el mismo.
- El Grupo de Respuesta a Incidentes es el responsable de:
    a) La investigación, gestión y solución de los incidentes de seguridad de la Información.
    b) Realizar el levantamiento de información y material que sirva de soporte o prueba de una investigación.
    c) Garantizar la retención segura de toda la información perteneciente al incidente para un análisis posterior (de ser necesario).
    d) Definir el plan de trabajo la implantación de las acciones correctivas requeridas, de acuerdo con los daños evidenciados en la investigación del incidente.
    e) Documentar en la base de conocimiento todas las medidas, actividades y tareas realizadas durante la gestión del incidente, de acuerdo a requerimiento regulatorios y legales que apliquen.
    f) El GRI debe estar disponible para atender los llamados que realice el *Líder del Equipo de respuesta a incidentes*, cuando se identifique o se sospeche que se ha producido un incidente y que de acuerdo a la severidad asignada deba ser atendido y gestionado por el GRI.
- El *Equipo de respuesta a incidentes (GRI)* será convocado por parte del *Líder Equipo de Respuesta a Incidentes*, para el tratamiento y atención de incidentes con una severidad de Crítico o Alto.
- Los incidentes de seguridad de la información con una severidad de Medio y Bajo, serán atendidos y tratados directamente por el *Líder Gestión de Incidentes, el Líder Equipo de Respuesta a Incidentes y/o Gestor Incidentes*, por lo tanto, no se convocará el *Grupo de Respuesta a Incidentes (GRI).*
- La información de la Gestión de Incidentes de Seguridad, así como las investigaciones realizadas es de carácter confidencial para la Universidad y su divulgación o distribución está bajo la responsabilidad del Líder de la Gestión de Incidentes en la Universidad EAN, siguiendo las directrices establecidos por la Universidad para emitir comunicaciones externas.

LINEAMIENTOS DE SEGURIDAD PARA INGRESO AL DATACENTER

Identificación y autenticación

El usuario se debe identificar cuando acceda a la infraestructura del Datacenter; si el ingreso es físico deberá identificarse por medio de una tarjeta de acceso previamente autorizada y asignada. Si el ingreso es lógico se debe identificar con las credenciales de acceso asignadas.

Administración del datacenter

Es responsabilidad de la Gerencia de Innovación y Desarrollo de TIC garantizar la seguridad para el ingreso al datacenter.

Acceso

El datacenter es un área de ACCESO RESTRINGIDO, es decir, el ingreso (de forma física o lógica) es exclusivo para funcionarios autorizados de la Universidad EAN, y/o terceros en cumplimiento de alguna labor específica previamente reportada y programada. Los funcionarios autorizados son:

- Gerente de Innovación y Desarrollo TIC o quien haga las veces.
- Coordinador de Datacenter
- Coordinador de infraestructura
- Personal de servicios generales (autorizado por la Gerencia de Innovación y Desarrollo TIC)
- Personal de vigilancia (en caso de emergencia)
- Terceros previamente autorizados y justificados por la Gerencia de Innovación y Desarrollo TIC

Las puertas de acceso a la sala del datacenter deben permanecer cerradas siempre (sin importar la hora o día), sólo deben activarse al ingreso del área utilizando las tarjetas de proximidad en el mecanismo electrónico respectivo. Adicionalmente, se deberá diligenciar la bitácora de acceso respectiva, lo cual será responsabilidad del funcionario acompañante y que realiza la apertura del datacenter.

El acceso físico, sólo es para los siguientes casos:

- Instalación, actualización, monitoreo, revisión o retiro de hardware, software e infraestructura del datacenter.
- Mantenimiento de la infraestructura de redes y comunicaciones.
- Visitas de terceros autorizados para labores de adquisición, mantenimiento, cotización, diagnóstico, auditorias y/o solicitudes especiales previamente autorizadas por la Gerencia de Innovación y Desarrollo TIC

El acceso lógico, está determinado para todos los casos en los que es necesario establecer conexión remota con algún dispositivo del datacenter. Tener en cuenta las condiciones que deben cumplir los proveedores en cuanto a usuarios y contraseñas definidos en este manual.

Monitoreo y control

- Se tienen cámaras de vigilancia continua. Estas deben registrar todas las actividades llevadas a cabo en el datacenter por el personal que tiene acceso y sus registros deben ser comparados con los registros de la tarjeta y la bitácora de acceso.
- La infraestructura del datacenter debe estar acorde a las necesidades de los equipos de cómputo y equipos activos de la red.
- El sistema contra incendio que contiene el gas Ecaro-25, debe ser verificado cada seis (6) meses.
- Las conexiones eléctricas que se vayan a realizar al interior del datacenter, deben tener la autorización y supervisión del personal técnico de la Gerencia de Innovación y Desarrollo de TIC.

Registro de las actividades y acciones del personal

- Para el caso de proveedores externos deberán tener un plan de las actividades a realizar y estos a su vez deben ser supervisados por el personal de la Gerencia de Innovación y Desarrollo de TIC.

- Se deberá definir y hacer uso de la bitácora de acceso físico al datacenter, la cual contendrá como mínimo los siguientes campos:

    - Fecha ingreso
    - Fecha salida
    - Hora ingreso
    - Hora salida
    - Identificación
    - Nombres y Apellidos
    - Empresa o proceso
    - Actividad a desarrollar
    - Firma
    - Colaborador TIC que acompaña (en los casos de ingreso de terceros)

- Cada tres (3) meses, el coordinador o profesional de apoyo a la gestión de seguridad de la información de la Gerencia de Innovación y Desarrollo de TIC recopilara los registros diligenciados de la Bitácora de acceso y los digitalizara para almacenarlos en el archivo (físico y digital).

Normas de Seguridad

El personal que por su función o actividad requiere de acceso al datacenter, deberá acatar las siguientes normas:

- No portar armas de fuego, cuchillos o similares
- No estar bajo estado de embriaguez o consumo de bebidas alcohólicas, cualquier droga o sustancia alucinógena
- No portar cámaras fotográficas y/o filmadoras sin autorización
- Mantener cerradas las puertas de acceso y demás áreas internas
- No introducir material magnético
- No arrastrar ningún objeto sobre el piso falso
- No introducir líquidos, alimentos y bebidas a las instalaciones
- No fumar
- Portar en todo momento el carné de identificación
- Acatar las normas establecidas en el presente manual

LINEAMIENTOS DE SEGURIDAD PARA LA INFRAESTRUCTURA TECNOLÓGICA

Mantenimiento preventivo y correctivo

- Es obligación de la Gerencia de Innovación y Desarrollo de TIC garantizar el correcto funcionamiento de los equipos de cómputo, razón por la cual desde allí se concretan tiempos de mantenimiento de los equipos con los colaboradores.
- El mantenimiento se realiza de acuerdo con los procedimientos definidos en el marco del sistema de gestión de la calidad institucional.

Infraestructura del Datacenter

- La infraestructura del Datacenter está a cargo de la Gerencia de innovación y Desarrollo de TIC, por lo tanto, desde este proceso se desarrollarán las acciones para garantizar la operación permanente de los servidores alojados allí, de igual forma se protege la información almacenada en los sistemas de almacenamiento, para que esté segura y disponible.
- El uso de los servidores del Datacenter está limitado para la instalación de servicios de tecnología de la Universidad EAN bajo la responsabilidad de la Gerencia de Innovación y Desarrollo de TIC
- Se realizará mantenimiento preventivo a los servidores del Datacenter, por lo menos una (1) vez al año y de acuerdo al procedimiento establecido por la Gerencia de Innovación y Desarrollo de TIC, según el calendario académico.

Renovación tecnológica y reposición de equipos

- La reposición de equipos consiste en la asignación de un equipo diferente al asignado inicialmente al colaborador cuando por fallas mayores éste quede inservible o cuando le sea hurtado. En este último caso el colaborador presenta la denuncia ante las autoridades competentes.
- La renovación tecnológica consiste en la asignación de un equipo nuevo por obsolescencia la cual se define de acuerdo con los siguientes criterios:

EQUIPO	CRITERIO DE OBSOLESCENCIA
Computador personal de escritorio	Tres años después de su compra y y/o puesta en operación. Se puede extender un año más dependiendo de su estado y soporte por parte del fabricante.
Computador personal portátil	Tres años después de su compra y/o puesta en operación. Se puede extender un año más dependiendo de su estado y soporte por parte del fabricante.
Servidor	Cinco años después de su compra y/o puesta en operación. Se puede extender de acuerdo al soporte ofrecido por el fabricante.
Switch	Cinco años después de su compra y/o puesta en operación. Se puede extender de acuerdo al soporte ofrecido por el fabricante.
Access Point	Tres años después de su compra y/o puesta en operación. Se puede extender de acuerdo al soporte ofrecido por el fabricante.
Sistema de almacenamiento	Tres años después de su compra y/o puesta en operación. Se puede extender de acuerdo al soporte ofrecido por el fabricante.
Disco externo	Dos años después de su compra y/o puesta en operación. Se puede extender de acuerdo al soporte ofrecido por el fabricante.
Equipos activos	Cinco años después de su compra y/o puesta en operación. Se puede extender de acuerdo al soporte ofrecido por el fabricante.
Teléfonos y accesorios	Cuando los dispositivos dejen de ser funcionales

- La renovación tecnológica se realizará con base en la disponibilidad presupuestal de la Universidad EAN, en el período específico.

Asignación de equipos de cómputo a colaboradores

- La Gerencia de Innovación y Desarrollo de TIC es la encargada de administrar y asignar los equipos de cómputo, periféricos y equipos de comunicación (telefonía local) a los colaboradores y docentes que requieran éstos recursos. Dicha asignación se realiza una vez la Gerencia de Desarrollo Humano notifica la formalización de la relación contractual, el cargo a desempeñar, el nombre del colaborador o docente y el tipo de contrato.

- El uso del equipo de cómputo asignado es personal e intransferible, es utilizado para realizar actividades institucionales. Por lo tanto, el colaborador asume responsabilidad en forma expresa de su uso o por parte de terceros.
- El equipo asignado es entregado al colaborador con las aplicaciones y software requerido de acuerdo al cargo y el tipo de contrato.
- La Gerencia de Innovación y Desarrollo de TIC establece controles de protectores de pantalla para que después de 30 minutos de inactividad del usuario, se bloquee para evitar accesos no autorizados.

Préstamo de equipos a estudiantes y docentes

La Universidad EAN tiene equipos de cómputo para préstamo a estudiantes y docentes, este servicio se presta en las salas de cómputo con equipos de escritorio y en las oficinas de audiovisuales y biblioteca con el préstamo de equipos portátiles. Quien haga uso de este servicio atiende los siguientes lineamientos:

- El servicio de préstamo de equipos de cómputo portátiles no incluye préstamo domiciliario, por lo tanto, no está autorizado sacar los equipos prestados de las instalaciones de la Universidad.
- El préstamo de equipos de las salas de cómputo está sujeto a la disponibilidad de cada sala, durante las clases programadas que hagan uso de estos recursos no se prestan los equipos.
- Los equipos dados en calidad de préstamo serán entregados con: el software base (Sistema Operativo), Software de ofimática (Suite de Office) y al menos un navegador de Internet con los complementos necesarios para la navegación.
- La instalación de software está restringida en los equipos de cómputo para préstamo.
- El retiro o remplazo de partes del equipo se considerará como un acto abusivo por parte del beneficiario del préstamo y será sancionado conforme a la normatividad interna vigente.
- En caso de pérdida del equipo prestado, el beneficiario del préstamo notifica el hecho ante las autoridades competentes, con copia a la Gerencia de Innovación y Desarrollo de TIC, para no generar multas y hacer la reposición por un equipo de similares características.
- En caso de daño parcial del equipo prestado por mal uso y/o mala manipulación, el beneficiario del préstamo asume los costos de la reparación.
- En caso de daño total del equipo prestado por mal uso y/o mala manipulación, el beneficiario del préstamo hace la reposición por un equipo de similares características.
- La Resolución No. 57 de 2015 fija los valores por concepto de sanciones pecuniarias a los usuarios de Biblioteca y Audiovisuales de la Universidad EAN por retraso, pérdida o daño en equipos de cómputo.

Equipos de cómputo de contratistas y proveedores

- Los equipos de cómputo propiedad de contratistas o proveedores que estén ubicados en las instalaciones de la Universidad EAN, deben contar con las respectivas licencias de software para las aplicaciones. En caso de incumplimiento de lo anterior, el contratista o proveedor asume las implicaciones legales del caso.
- Las labores de mantenimiento y soporte de los equipos de cómputo propiedad de contratistas o proveedores que estén ubicados en las instalaciones de la Universidad EAN, no serán atendidas por la Gerencia de Innovación y Desarrollo de TIC salvo en aquellos equipos en los cuales la relación contractual definida con el tercero lo especifique.

- El acceso a la red de datos de la Universidad EAN de los equipos de cómputo propiedad de contratistas o proveedores que estén ubicados en las instalaciones de la Universidad EAN, sólo se permite si éstos cuentan con software antivirus, antispyware licenciados, actualizados y con las actualizaciones de seguridad del sistema operativo.
- El acceso a Internet de los equipos de cómputo propiedad de contratistas o proveedores que estén ubicados en las instalaciones de la Universidad EAN, será restringido, excepto en aquellos casos que la relación contractual definida con el tercero lo especifique.

Equipos que ingresan a la Universidad EAN

- La Universidad EAN no asume responsabilidad alguna, sobre los equipos de cómputo que ingresen a sus instalaciones y que no hayan sido asignados por la Gerencia de Innovación y Desarrollo de TIC.

Instalación de Software

- No se permite la instalación de software diferente al que se le entrega con el equipo de cómputo. Es facultad exclusiva de la Gerencia de Innovación y Desarrollo de TIC realizar la instalación de software en los equipos de cómputo de la Universidad EAN.
- La instalación de software adicional, es una actividad exclusiva de la Gerencia de Innovación y Desarrollo de TIC, con el fin de gestionar las licencias de software propiedad de la Universidad EAN.
- Para la instalación de software especializado o adicional al que se entrega con el equipo de cómputo se hace la solicitud a través de la mesa de servicio a la Gerencia de Innovación y Desarrollo de TIC, aun cuando se trate de software con licenciamiento libre.
- No se instalan licencias propiedad del colaborador o de alguna otra entidad sin la autorización de la Gerencia de Innovación y Desarrollo de TIC.
- La copia de archivos de música y video en los equipos de la Universidad está restringida, únicamente son válidos para uso académico en cumplimiento con el reglamento de propiedad intelectual vigente por la Universidad EAN.

Instalación o retiro de hardware

- Es facultad exclusiva de la Gerencia de Innovación y Desarrollo de TIC realizar la instalación o retiro en los equipos de cómputo de la Universidad EAN de partes como: tarjetas de memoria RAM, tarjetas de red, tarjetas de video, discos duros internos, procesadores, tarjetas modem, tarjetas video, entre otros.
- La instalación de hardware adicional al que se entrega con el equipo de cómputo es una actividad restringida para los colaboradores con excepción de los dispositivos de audio, micrófonos externos, memorias USB o Discos externos (Ver 2.3. Lineamientos de Seguridad para los Medios de almacenamiento extraíbles)
- La instalación de impresoras se realizará por parte de la empresa que tenga asignado el contrato para la gestión de impresión en la Universidad EAN, a este contratista se le otorgará los privilegios para instalación sin perjuicio de las cláusulas de confidencialidad definidas para la relación contractual con el proveedor. Se exceptúan las áreas que tienen impresoras que son de propiedad de la Universidad EAN.
- Cuando se presente retiro del colaborador/docente se procederá de la siguiente forma:

- En caso de tener asignado un equipo de cómputo portátil y otros elementos de tecnología, el colaborador debe hacer entrega de los mismos a la Gerencia de Innovación y Desarrollo de TIC para legalizar paz y salvo.
- Si el colaborador tiene asignado un equipo de cómputo de escritorio y otros elementos de tecnología, se verificará el estado de los elementos para poder legalizar paz y salvo, y si transcurrida una semana no se ha realizado reposición del cargo se procederá a recoger el equipo de cómputo. En caso de requerir el equipo de cómputo en el área por más tiempo, el líder de proceso deberá notificarlo y el activo será asignado a él.

Información almacenada en la infraestructura tecnológica

- La información contenida en los discos duros internos de los equipos de cómputo y los dispositivos de almacenamiento externos, es propiedad de la Universidad EAN. (Ver 2.3 Lineamientos de Seguridad para los Medios de almacenamiento extraíbles)
- Cada colaborador tiene acceso a los repositorios institucionales, según sea el caso, para salvaguardar la información sensible o confidencial (Ver 2.7 Lineamientos de Seguridad para la Clasificación, Reciclaje y/o Destrucción de la información); solo de esta manera la Gerencia de Innovación y Desarrollo de TIC garantizará las copias de respaldo a la información.
- No está permitido guardar, descargar archivos en los discos duros internos o dispositivos de almacenamiento externo asignados por la Universidad EAN, que correspondan a formatos de música, libros electrónicos videos o películas cuya propiedad intelectual o titularidad de derechos de autor no haya sido cedida a la Universidad EAN o adquirida por ésta.
- La información de los correos electrónicos de los colaboradores no se incluye en las copias de respaldo, por lo tanto, es responsabilidad de cada colaborador tomar las acciones correspondientes y asumir buenas prácticas para la gestión de su cuenta de correo. (Ver 2.2. Lineamientos de Seguridad para el Correo Electrónico)

Acceso a la Red de datos

- El ingreso a la red de datos de la Universidad EAN se realiza a través del usuario y la contraseña que se le asigna al colaborador, docente o estudiante para el ingreso al equipo de cómputo, los recursos informáticos y sistemas de información.
- El acceso a los equipos de cómputo y/o servidores de la Universidad EAN desde fuera de sus instalaciones sólo será permitido a las personas autorizadas por el líder del proceso y la Gerencia de Innovación y Desarrollo de TIC o quien haga las veces, y se hará a través del establecimiento de redes privadas virtuales (VPN), para los Teletrabajadores o colaboradores autorizados. Ver apartado 2.1.1.1 Acceso a la red de datos.
- La red de datos de la Universidad EAN es de uso estrictamente laboral y académico. Es responsabilidad del usuario tener buenas prácticas para el cuidado, preservación, buen uso y protección de la información.
- Se considera falta grave el hecho de que cualquier persona capture información, realice grabación de conversaciones telefónicas o de chat sin previa autorización, accediendo a las redes de datos de la Universidad.
- Se permitirá el acceso remoto a los equipos de cómputo dentro de las instalaciones de la Universidad EAN, para actividades de soporte técnico previo consentimiento del usuario al cual se asignó el equipo y bajo la supervisión de la Gerencia de Innovación y Desarrollo de TIC.

Navegación en Internet

- El acceso a Internet a través de los navegadores es exclusivamente con fines laborales de acuerdo a las actividades del colaborador.
- El acceso a las plataformas de redes sociales para los colaboradores, está permitido de manera controlada.
- Acceder a la red institucional, para cometer delitos será sancionado conforme a la normatividad interna y denunciado ante las autoridades del orden nacional competentes.
- El acceso a Internet desde la red inalámbrica es exclusivo para estudiantes, docentes, colaboradores e invitados, a estos últimos se le suministrará las credenciales de acceso al momento de estar en las instalaciones de la Universidad.
- La Universidad EAN podrá monitorear el tráfico de los equipos que ingresan a la red y ante situaciones de tráfico sospechoso se limitará el acceso y navegación de las máquinas comprometidas.

LINEAMIENTOS DE SEGURIDAD PARA PROVEEDORES O TERCEROS

Descripción

La Universidad EAN contempla lineamientos de seguridad para todas las partes interesadas incluyendo los proveedores o terceros, en este apartado se establecen las obligaciones que deben ser cumplidas por proveedores y terceros que tengan algún vínculo con la institución. Adicional se tiene en cuenta los acuerdos de nivel de servicio, cumplimiento, confidencialidad, transmisión de datos y demás directrices que se establezcan en el proceso de contratación.

Lineamientos de ingreso de equipos portátiles y escritorio remoto

- El proveedor o tercero deberá presentar a la Gerencia de Innovación y Desarrollo de TIC la solicitud del usuario de red para realizar sus labores teniendo en cuenta las consideraciones de este manual y el contrato.
- El proveedor o tercero tiene acceso controlado a los sistemas de información que soporta y el TIC considere pertinente, siempre y cuando se documenten los procedimientos ejecutados y se valide la viabilidad de su ejecución con el respectivo líder técnico, adicionalmente si se requiere acceso remoto se realiza en lo posible mediante herramientas de escritorio remoto y el acompañamiento de un colaborador adscrito a la Gerencia de Innovación y Desarrollo de TIC.

Lineamientos generales

Se prohíbe a los proveedores o terceros que guarden alguna relación con la universidad EAN, cuando tengan acceso a la red o a los centros de cómputo de la universidad, las siguientes conductas:

- La descarga de programas, fotos, música, videos y demás tipo de información digital vía Internet, al igual que del tráfico de información vía mensajería instantánea, a excepción de los medios autorizados por la compañía.
- Instalar en los equipos cualquier Software no autorizado, sin importar su modo de distribución, ya sea electrónica o físicamente.
- Compartir carpetas, transferir archivos por la red ya sea por correo electrónico o cualquier otro medio de comunicación, con fines diferentes a los laborales, ya sea para diversión, intrusión o cualquier otro tipo de interés.

- Dañar física o lógicamente los equipos o la infraestructura informática
- Conectar, desconectar, desmantelar, retirar o cambiar partes, reubicar equipos o cambiar de configuración a los mismos sin autorización expresa de la Gerencia de Innovación y Desarrollo de TIC de la universidad EAN.
- Instalar dispositivos o tarjetas de acceso remoto, módems, RDSI, routers o cualquier otro dispositivo de comunicaciones en los equipos e infraestructura tecnológica destinados para la prestación del servicio sin la debida autorización de la Gerencia de Innovación y Desarrollo de TIC de la universidad EAN.
- Usar equipos o cuentas de equipos de red sin autorización de la Gerencia de Innovación y Desarrollo de TIC.
- Realizar cualquier acto que interfiera en el correcto funcionamiento de los equipos informáticos o de la infraestructura tecnológica para la prestación del servicio, estaciones de trabajo de escritorio, portátiles, equipos terminales de telefonía, terminales de comunicaciones alámbricas, terminales de comunicación inalámbricas, equipos periféricos, red de comunicaciones, canal de comunicaciones de voz, datos o Internet.
- Instalar o ejecutar programas que perjudiquen la estabilidad de los equipos, su sistema operativo, sus programas internos y aplicaciones. Esto incluye los programas conocidos como virus informáticos, cualquier tipo de ensayo o experimento, hardware, software, spammers, spimmers, troyanos, keyloggers, entre otros.
- Uso del servicio de manera tal que constituya una molestia, abuso, amenaza o que de cualquier forma atente contra la integridad del equipo e infraestructura tecnológica.
- Extraer información física o electrónica que viole los derechos de autor y/o la confidencialidad de la universidad EAN, sus clientes o sus proveedores.
- Instalar o ejecutar programas que traten de descubrir la información distinta de la del propio usuario. Esto incluye los sniffer, scanner de puerto, analizador de protocolos, detectores de redes, herramientas de ping, DOS, entre otros.
- Intentar sobrepasar protecciones de datos o sistemas de seguridad informática.
- Hacer uso abusivo de las claves o permisos que posea en virtud de cualquier tipo de relación con la universidad EAN, para fines particulares o beneficio de terceros o para acceder a información de equipos ajenos.
- Uso de equipos portátiles propios, para acceso a los recursos tecnológicos de la universidad EAN, sin previa autorización.
- Uso de los recursos de correo electrónico, impresoras, fax, scanner, y demás herramientas informáticas para fines que no corresponden al objeto de la relación con la universidad EAN.
- Aplicar el procedimiento para control de cambios establecido por la universidad.

LINEAMIENTOS DE SEGURIDAD PARA LA ADQUISICIÓN DE SERVICIOS DE CLOUD COMPUTING Y HOSTING

Descripción

La Universidad EAN ha adoptado modalidades de contratación de servicios asociados con la adquisición y prestación de servicios en ambientes de *Cloud Computing (Computación en la Nube)* y/o *Hosting,* por lo tanto, se deben establecer los lineamientos específicos de seguridad de la información asociados a éstos ambientes con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos de información de la Universidad involucrados.

Lineamientos Generales

- Son responsables del cumplimiento de la presente política específica, las áreas encargadas de realizar total o parcialmente una o más de las siguientes actividades:
    a. Dirigir, administrar, controlar, implementar, o cualquier otra actividad relacionada con el desarrollo de proyectos que incluyan la prestación de servicios de Cloud Computing y/o Hosting.
    b. Gestionar proyectos para la adquisición o mejoramiento de sistemas de información y/o plataformas y software de Cloud Computing y Hosting.
    c. Gestionar, autorizar, proveer, administrar, monitorear, configurar o cualquier otra actividad relacionada con el acceso, procesamiento, transmisión o almacenamiento de información y/o el uso de componentes tecnológicos y/o sistemas de La Universidad EAN por parte de terceros en servicios de Cloud Computing y/o Hosting.
- Para el despliegue e implementación de servicios en Cloud Computing y/o Hosting se deben tener en cuenta los requerimientos y lineamientos de seguridad establecidos por la Gerencia de Innovación y Desarrollo de TIC de la Vicerrectoría Financiera de la Universidad o quién ésta última designe, de acuerdo a la siguiente información (sin limitarse a):
- Previo a la contratación, se deben establecer los requisitos de seguridad de la información con los Terceros que tengan acceso a la información y activos tecnológicos de la Universidad, de acuerdo a la clasificación de la información, los requerimientos de las regulaciones locales e internacionales que apliquen o la evaluación de riesgos de TI (si existiere).
- Todo proyecto de Cloud Computing y Hosting debe ser documentado, especificando los servicios y/o sistemas de información que se alojaran en dichos ambientes con la descripción de los modelos de servicio a implementar y deberá contar con aprobación del esquema de gobierno de la Universidad (Comité de Seguridad).
- El proveedor de Servicios de Cloud Computing y/o Hosting debe tener en funcionamiento una organización responsable de la seguridad de la información, en la que se defina los roles y responsabilidades frente a la seguridad de la información y deberá definir un rol dentro de la Organización que sea el punto de contacto oficial para todos los temas relacionados con la Seguridad de la Información que es de alcance del servicio contratado.
- En el momento de reemplazo / dada de baja un sistema o componente tecnológico (físico o virtual) del servicio de Cloud y/o Hosting contratado, la información almacenada en él debe eliminarse utilizando técnicas de borrado seguro aprobadas por la Universidad EAN.
- El proveedor debe garantizar la realización de copias de respaldo periódicas a los datos que se encuentran en el alcance del servicio contratado y en el formato utilizado, definido y aprobado por La Universidad EAN (el formato del backup no debe ser exclusivo del proveedor del servicio contratado), de manera que permitan trasladar y recuperar la información sin depender de costos y operación del proveedor del servicio cuando se determine cambiar de proveedor, o retomar la información y/o aplicaciones involucradas en el servicio. Esta política o lineamiento también incluye o aplica para la migración de información relacionada con copias de registros, registros de acceso y otra información pertinente que pueda requerirse para las cuestiones legales y de cumplimiento.
- El proveedor de servicio deberá tener implementado un sistema de gestión de riesgo de seguridad de la información, comunicando a la Universidad de manera periódica sobre el análisis de los controles establecidos, así como de los planes o medidas de mitigación de los riesgos identificados
- El proveedor debe garantizar que los datos solo se almacenan en ubicaciones permitidas en el contrato, en Acuerdos de niveles de servicio (SLA´s) y/o en requerimientos sujetos a cumplimiento nacionales o internacionales, sin mezclar la información de la Universidad con información de otros

clientes durante su uso, almacenamiento o tránsito, esto relacionado con la seguridad de la información y la geo-localización de los datos.

- El proveedor debe establecer mecanismos que permitan contar con conexiones seguras de entre La Universidad y las aplicaciones y/o servicios ofrecidos por el proveedor.
- La Universidad y el proveedor deben establecer roles o niveles de acceso de acuerdo a las actividades, responsabilidades y necesidades de los diferentes usuarios; y se deben otorgar permisos de acceso a los recursos informáticos en función de los roles definidos.
- La Universidad EAN debe realizar una revisión periódica de cuentas de usuario. Los accesos a los diferentes recursos de Información deben ser monitoreados y revisados como mínimo semestralmente por el administrador, dueño de la Información o a quien designe, con el fin de asegurar que los niveles de acceso otorgados son apropiados y están siendo utilizados de manera correcta.
- Se debe conocer y definir la ubicación de los datos que son del alcance del servicio contratado. Conocer y definir la ubicación de los datos para validar la conveniencia de su ubicación al cumplir aspectos legales aplicables al país donde se encuentren los mismos, la jurisdicción, condiciones exigibles para que la transferencia de los datos a los sistemas del proveedor pueda ser viable evitando tener potenciales inconvenientes legales y de acceso (autorizado o no) a la información.
- Se debe restringir el movimiento de los activos de información de La Universidad EAN sólo a ubicaciones geográficas conformes con el cumplimiento de los requerimientos legales o regulatorios aplicables a La Universidad EAN.
- Siempre que el proveedor de servicios de Cloud Computing Y/O Hosting pretenda realizar movimiento de información a una ubicación geográfica (país) distinta a la inicialmente aprobada y contratada por la Universidad EAN, deberá informar formalmente su intención y La universidad quién después de analizar su conveniencia, oportunidad y cumplimiento de los requerimientos establecidos para el servicio (incluyendo los presentes lineamientos) podrá aprobar o no dicho movimiento.
- LA Universidad EAN es el dueño de la información a ser procesada por el proveedor independientemente del modelo de despliegue o de servicio de Cloud Computing y/o Hosting contratado.
- Contractualmente se deben definir y formalizar las penalidades o sanciones al proveedor de Servicios de Cloud Computing y/o Hosting en caso de incumplir con regulaciones, leyes o normativas aplicables al servicio contratado o a la información del alcance del mismo
- La Universidad y el proveedor de Cloud y/o Hosting deben establecer las funciones y responsabilidades que le corresponden en materia de e-Discovery. Las partes deben comprender mutuamente las funciones y responsabilidades de cada uno en relación al e-Discovery, incluyendo actividades como la preservación de documentos debido a litigio, búsquedas de descubrimiento, prestación de testimonio experto, etc.
- La Universidad EAN y el proveedor deben acordar y aprobar formalmente un proceso unificado para responder a citaciones, notificaciones, emplazamientos y otras solicitudes legales que les puedan ser realizadas con alcance a la información o datos involucrados en la prestación del servicio contratado o por motivo o alcance diferente
- Se deberán establecer requerimientos contractuales para que La Universidad EAN realice auditorias, al menos una vez al año, con o sin programación previa al proveedor del servicio; con el fin de evaluar las capacidades de seguridad del proveedor de Cloud Computing y/o Hosting. La Universidad podrá delegar dicho proceso de auditoría en un tercero.
- La Universidad EAN debe establecer requerimientos contractuales con el fin coordinar con el proveedor Cloud Computing y/o Hosting la ejecución de pruebas de vulnerabilidad a los recursos involucrados en la prestación del servicio.

- La información de las bases de datos en soluciones sobre Cloud y/o Hosting debe ser protegida mediante el uso de mecanismos de cifrado.
- La información confidencial y/o bajo cumplimiento normativo o legal y en los casos que lo requiera, debe ser cifrada tanto en reposo como en tránsito y debe permanecer de esta forma en los medios de respaldo.
- Para el cifrado con mecanismos propios u ofrecidos por el Proveedor de Cloud Computing y/o Hosting, se debe contar con procesos formalizados y en funcionamiento para el ciclo de vida de la gestión de llaves. El proceso de gestión debe contemplar (sin limitarse a) la creación, uso, almacenamiento, respaldo, recuperación y eliminación segura de claves utilizadas para el cifrado de datos.
- El Proveedor de Cloud Computing y/o Hosting debe emplear una llave de cifrado diferente para cada cliente de sus servicios.
- El proveedor Cloud Computing y/o Hosting debe ofrecer varias opciones de autenticación fuerte tales como contraseñas de un solo uso, biométricas, certificados digitales, etc. que puedan ser utilizadas en la prestación del servicio.
- El proveedor de Servicios de Cloud Computing y/o Hosting deberá tener en operación un proceso de gestión de Incidentes de Seguridad Informática y de la Información, el cual debe ser alineado y aprobado por la Universidad EAN.
- El proveedor deberá contar con planes de recuperación ante desastres documentados, implementados y probados y deberán incluir escenarios específicos para La Universidad EAN, así como contemplar escenarios de perdida de continuidad en la prestación de servicios por parte de los terceros del proveedor de Cloud Computing y/o Hosting.
- La Universidad EAN periódicamente debe revisar, verificar y validar los planes de Continuidad de Negocio y de Recuperación de desastres ofrecidos por el proveedor de servicio de Cloud Computing y/o Hosting.

LINEAMIENTOS DE SEGURIDAD PARA PROYECTOS

Descripción

Como parte del desarrollo de sus actividades la Universidad ejecuta proyectos para la adquisición e implementación de elementos que permitan mejorar la prestación y desarrollo de los servicios que ofrece la Institución. Por ello es de vital importancia implementar como parte de los proyectos aspectos de seguridad que faciliten su seguimiento y el aseguramiento de la información institucional.

Lineamientos generales

Los siguientes son puntos de cumplimiento para todos los proyectos que se desarrollen en la Universidad:

- Incluir como parte de la formulación del proyecto la identificación y gestión de los riesgos asociados a la seguridad de la información para establecer controles para el tratamiento adecuado de la información a emplear en todas las etapas del proyecto.
- Identificar la legislación en materia de seguridad de la información aplicable al proyecto y definir los planes para dar cumplimiento integrándolos durante la ejecución del proyecto.
- Establecer canales de comunicación seguros para intercambio de información con partes internas y externos de acuerdo a la sensibilidad de la información a manejar en las etapas del proyecto.

- Establecer como parte de los contratos / OPS / orden de compra u otra forma de acuerdo de prestación de servicios, productos prototipos, las cláusulas de confidencialidad y seguridad de la información establecidas por el área jurídica y las presentes en el lineamiento 2.11 lineamientos de seguridad para proveedores o terceros y 2.14 Administración de datos personales.
- Incluir como parte de la gestión del proyecto, esquemas de control de cambios para asegurar la trazabilidad en el desarrollo del proyecto.

A nivel de proyectos tecnológicos que implican el desarrollo o adquisición de software:

- Validar y asegurar que el desarrollo sigue buenas prácticas a nivel de desarrollo seguro.
- Incluir como parte de los requerimientos no funcionales, la realización de pruebas de seguridad al software adquirido o desarrollado.

LINEAMIENTOS DE SEGURIDAD PARA FIRMA DIGITAL

Descripción

A partir del uso de firmas digitales la Universidad EAN busca otorgar la validez jurídica a los documentos y certificaciones que expida digitalmente.

Lineamientos generales

Para el trámite, solicitud, adquisición, revocación de firmas digitales a nombre de la Universidad deben ser considerados los siguientes aspectos:

- Toda solicitud de adquisición, revocación o reposición de firmas digitales está a cargo de la Gerencia de Innovación y Desarrollo de TIC.
- Los colaboradores que cuentan con firma digital o certificados como representantes jurídicos deben tramitar la solicitud a través de la Gerencia de Innovación y Desarrollo de TIC, quien es el único enlace para el trámite con la entidad de certificación.
- La solicitud de adquisición de firma digital o certificados como persona jurídica representante de la Universidad debe ser validados por Secretaria General como ente jurídico de la Universidad.

LINEAMIENTOS ADMINISTRACIÓN DE DATOS PERSONALES (HABEAS DATA)

Medidas de seguridad comunes

Estas medidas de seguridad aplican para todo tipo de datos: públicos, semiprivados, privados, sensibles de acuerdo con la definición establecida en la Ley Estatutaria 1581 de 2012, que se encuentren en bases de datos automatizadas o no automatizadas en la Universidad EAN.

Los responsables nombrados de las bases de datos no automatizadas serán los encargados de asegurar el cumplimiento de los controles aplicables a las mismas y descritas dentro de este manual en el numeral 0. Para las bases de datos automatizadas la Gerencia de Innovación y Desarrollo de TIC apoyará la implementación de los controles.

Gestión de documentos y soportes

Los documentos y soportes en los que se encuentran las bases de datos se determinan en el inventario de documentos y soportes.

Los responsables del tratamiento de las bases de datos son los encargados de vigilar y controlar que personas no autorizadas, no puedan acceder a los documentos y soportes con datos personales.

Los documentos y soportes deben ser clasificados según el tipo de información que contienen, ser inventariados y ser accesibles solo por el personal autorizado, salvo que las características de los mismos hagan imposible la identificación referida, en cuyo caso se dejará constancia motivada en el registro de entrada y de salida de documentos y en documentos anexos al manual.

La identificación de los documentos y soportes que contengan datos personales sensibles debe realizarse utilizando sistemas de etiquetado comprensibles y con significado que permita a los usuarios autorizados identificar su contenido y que dificulten la identificación para el resto de personas.

La salida de documentos y soportes que contengan datos personales fuera de los locales que están bajo el control del responsable del tratamiento debe ser autorizada por este último. Este precepto también es aplicable a los documentos o soportes anexados y enviados por correo electrónico.

Control de acceso

El personal de la Universidad EAN solamente debe acceder a aquellos datos y recursos necesarios para el desarrollo de sus labores y sobre los cuales se encuentren autorizados por el responsable del tratamiento.

La Universidad EAN se ocupa del almacenamiento de una lista actualizada de usuarios, perfiles de usuarios, y de los accesos autorizados para cada uno de ellos. En el caso de soportes informáticos, puede consistir en la asignación de contraseñas, y en el caso de documentos, en la entrega de llaves o mecanismos de apertura de dispositivos de almacenamiento donde se archive la documentación.

La modificación sobre algún dato o información, así como la concesión, alteración, inclusión o anulación de los accesos autorizados y de los usuarios recogidos en la lista actualizada mencionada en el párrafo anterior, corresponde de manera exclusiva al personal autorizado.

Cualquier personal ajeno a la Universidad EAN, que, de forma autorizada y legal, tenga acceso a los recursos protegidos, estará sometido a las mismas condiciones y tendrá las mismas obligaciones de seguridad que el personal propio.

Ejecución del tratamiento fuera de los locales

El almacenamiento de datos personales del responsable del tratamiento o encargado del tratamiento en dispositivos portátiles y su tratamiento fuera de los locales requiere una autorización previa por parte de la Universidad EAN, y el cumplimiento de las garantías de seguridad correspondientes al tratamiento de este tipo de datos.

Bases de datos temporales, copias y reproducciones

Las bases de datos temporales o copias de documentos creadas para trabajos temporales o auxiliares deben cumplir con el mismo nivel de seguridad que corresponde a las bases de datos o documentos originales. Una vez que dejan de ser necesarias, estas bases de datos temporales o copias son borradas o destruidas, impidiéndose así el acceso o recuperación de la información que contienen.

Solamente el personal autorizado para realizar copias o reproducciones de bases de datos automatizadas corresponde a la Gerencia de Innovación y Desarrollo de TIC.

Medidas de seguridad para bases de datos no automatizadas

Los colaboradores de la Universidad EAN que tengan bajo su custodia bases de datos no automatizadas tendrán las obligaciones que a continuación se enuncian:

1. **Almacenamiento**

Garantizar el apropiado almacenamiento de la documentación física y digital en la cual reposan los datos objeto de tratamiento siguiendo los procedimientos adecuados para garantizar una correcta conservación, localización y consulta de la información, y que a su vez permitan el correcto ejercicio de los derechos de los Titulares consagrados en la ley.

2. **Control de acceso a documentos digitales y físicos.**

Usar en debida forma los dispositivos de almacenamiento digital con mecanismos apropiados y provistos por la Universidad EAN para evitar el acceso a la información en ellos contenida por personas no autorizadas.

Para los archivos físicos se deberán utilizar los muebles dispuestos por la Universidad como: archivadores, armarios u otros ubicados en áreas de acceso protegidas con llaves u otros controles que eviten el acceso a la información por personas no autorizadas.

En ambos casos, el acceso debe estar limitado únicamente a personal autorizado.

3. **Custodia de documentos**

Deber de diligencia y custodia durante la revisión o tramitación de los mismos. En caso de tener que compartir la información que está bajo su responsabilidad con otro proceso o colaborador de la Universidad EAN, el proceso solicitante deberá realizar dicha petición por medio escrito, explicando detalladamente cual será la actividad institucional a ser realizada con estos datos, verificando que se tenga autorización para ello de parte de los titulares y haciendo la debida consulta previa a la Secretaría General para su concepto favorable, de otro modo estarían incurriendo en un mal manejo de las bases de datos.

4. **Auditoria interna**

Realizar un informe de detección de deficiencias y propuesta de correcciones cuando note conveniente hacerlo, dicho informe deberá ser conservado por la Universidad EAN con el fin de ponerlo a disposición de la autoridad competente en caso de requerirlo. Dicho informe deberá realizarse mínimo una vez al año.

5. **Copia o reproducción**

La copia o reproducción de la información solo podrá realizarse por los usuarios debidamente autorizados y con fines específicos y legítimos dentro de las actividades de la Universidad EAN, posterior a esto y si no es necesaria su conservación se deberá proceder a la destrucción de dicha información de manera que impida su recuperación.

Auditorías

Las bases de datos que contengan datos personales, objeto de tratamiento por la Universidad EAN, se han de someter a auditorías internas o externas que verifiquen el cumplimiento de las medidas de seguridad contenidas en este manual. El alcance y periodicidad de las auditorías será definido por la Universidad en periodos anuales.

Serán objeto de auditoría los sistemas de información y las instalaciones de almacenamiento y tratamiento de datos de acuerdo a la estrategia que la Universidad defina para cada periodo anual.

Archivo de documentos

La Universidad EAN, fija los criterios y procedimientos de actuación que se deben utilizar para el archivo de documentos que contengan datos personales conforme a la Ley. Los criterios de archivo garantizan la conservación, localización y consulta de los documentos y hacen posible los derechos de consulta y reclamo de los Titulares.

Para los documentos que sean archivados se debe considerar, entre otros, criterios como el grado de utilización de los usuarios con acceso autorizado a los mismos, la actualidad de su gestión y/o tratamiento y la diferenciación entre bases de datos históricas y de administración o gestión de la universidad.

Los dispositivos de almacenamiento de documentos deben disponer de llaves u otros mecanismos que dificulte su apertura, excepto cuando las características físicas de éstos lo impidan, en cuyo caso la Universidad EAN, adoptará las medidas necesarias para impedir el acceso de personas no autorizadas.

Cuando los documentos que contienen datos personales se encuentren en proceso de revisión o tramitación y, por tanto, fuera de su medio de almacenamiento, ya sea antes o después de su archivo, la persona que se encuentre a cargo de los mismos debe custodiarlos e impedir en todo caso que personas no autorizadas puedan acceder a ellos.

Los medios de almacenamiento que contengan documentos con datos personales clasificados con nivel de seguridad sensible, deben encontrarse en áreas o locales en las que el acceso esté protegido con puertas de acceso con sistemas de apertura de llave u otros mecanismos similares. Estas áreas deben permanecer cerradas cuando no se precise el acceso a dichos documentos.

Acceso a los documentos

El acceso a los documentos ha de realizarse exclusivamente por el personal autorizado por los responsables del tratamiento, siguiendo los mecanismos y procedimientos definidos.

El procedimiento de acceso a los documentos que contienen datos clasificados como sensibles implica el registro de accesos a la documentación, la identidad de quien accede, el momento en que se produce el acceso y los documentos a los que se han accedido. El acceso a documentos con este tipo de datos se realiza por personal autorizado; si se realiza por personas no autorizadas deberá ser reportado como un incidente de seguridad.

Medidas de seguridad para bases de datos automatizadas

Identificación y autenticación.

La Universidad EAN, debe instalar un sistema de seguridad informática que permita identificar y autenticar de forma correcta a los usuarios de los sistemas de información, con el fin de garantizar que solo el personal autorizado pueda acceder a las bases de datos.

También ha de establecer un mecanismo que permita la identificación personalizada e inequívoca de todo usuario que intente acceder al sistema de información y que verifique si está autorizado. La identificación debe realizarse mediante un sistema único para cada usuario que accede a la información teniendo en cuenta el nombre de usuario, la identificación de empleado, el nombre del área o proceso, etc.

Para los sistemas de autenticación basados en contraseña, se ha de cumplir con los lineamientos para contraseñas implementados en este manual.

Entrada y salida de documentos o soportes

La entrada o salida de documentos y/o soportes debe registrarse indicando el tipo de documento o soporte, la fecha y hora, el emisor y/o receptor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen según el nivel de seguridad, la forma de envío y la persona responsable de la recepción o envío.

La Universidad EAN o quien ésta designe, debe proporcionar los medios o sistemas de información para realizar el registro de entrada y/o salida de los documentos o soportes.

Copias de respaldo y recuperación de datos personales.

Todas las bases de datos deben tener una copia de respaldo a partir de las cuales se puedan recuperar los datos. (Revisar documento TIC-301 Generación y Restauración de Copias Respaldo).

De igual modo, ha establecido procedimientos para la recuperación de los datos con el objetivo de garantizar en todo momento la reconstrucción al estado en el que éstos se encontraban antes de su pérdida o destrucción. Cuando la pérdida o destrucción afecte a bases de datos parcialmente automatizadas se grabarán manualmente los datos dejando constancia de ello en este manual.

La Universidad EAN, se encargará de controlar el correcto funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y recuperación de los datos cada 6 meses. (Revisar documento TIC-301 Generación y Restauración de Copias Respaldo).

La Universidad EAN, debe conservar una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar distinto a aquel en el que se encuentren los equipos donde se lleva a cabo su tratamiento. Este lugar deberá cumplir en todo caso las mismas medidas de seguridad exigidas para los datos originales.

Registro de acceso

Los intentos de acceso a los sistemas de información de la Universidad EAN, deben guardar como mínimo, la identificación del usuario, la fecha y hora en que se lleva a cabo, la base de datos a la que se accede, el tipo de acceso y si ese acceso ha sido autorizado o no autorizado. En caso de que el registro haya sido autorizado, se guarda la información que permita identificar el registro consultado.

Los datos que contiene el registro de acceso deben conservarse de acuerdo con el periodo de retención definido por la Universidad y el cumplimiento de la legislación aplicable.

Redes de comunicaciones

El acceso a datos personales a través de redes de comunicaciones, públicas o privadas, debe someterse a medidas de seguridad equivalentes al acceso local de datos personales.

La transmisión de datos personales mediante redes públicas o inalámbricas de comunicaciones electrónicas se tiene que llevar a cabo cifrando dichos datos, o utilizando otro mecanismo similar que garantice que la información no sea inteligible ni manipulada por terceras personas.

Bases de datos y sistemas de información

Las bases de datos almacenadas y tratadas por la Universidad EAN, se recogen en la siguiente tabla, donde se indica el nivel de seguridad.

Base de datos	Nivel de seguridad	Sistema de tratamiento
Empleados	Sensibles	Mixto
Salud	Sensibles	Mixto
Alumnos	Sensibles	Mixto
Ex alumnos	Sensibles	Mixto
Biblioteca	Sensibles	Mixto
Proveedores	Básico	Mixto
Prospectos Alumnos	Básico	Mixto
Movilidad de estudiantes y profesores	Básico	Mixto
Educación no formal	Básico	Mixto
Prácticas	Sensibles	Mixto
Consejería	Sensibles	Mixto
Mercadeo	Básico	Mixto

Tabla Bases de datos y nivel de seguridad

*** Mixto:** Se refiere a bases de datos automatizadas y no automatizadas.

Medidas para el transporte, destrucción y reutilización de documentos y soportes

Cuando corresponda desechar cualquier documento (original, copia o reproducción) o soporte que contenga datos personales debe procederse a su destrucción o borrado, a través de la implementación de medidas orientadas a evitar el acceso o recuperación de la información contenida en dicho documento o soporte.

Cuando se lleve a cabo el traslado físico de documentos o soportes deben adoptar las medidas necesarias para impedir el acceso indebido, la manipulación, la sustracción o la pérdida de la información. El traslado de soportes que contengan datos personales se realiza cifrando la información, o utilizando cualquier otro mecanismo que garantice que no se manipule ni se acceda a la misma.

Los datos contenidos en dispositivos portátiles deben estar cifrados cuando se hallen fuera de las instalaciones que están bajo control de la Universidad EAN. Cuando no sea posible el cifrado, se debe evitar el tratamiento de datos personales mediante este tipo de dispositivos; sin embargo, se podrá proceder al tratamiento cuando sea estrictamente necesario, adoptando para ello medidas de seguridad que tengan en cuenta los riesgos e incluyéndolas en el presente manual.

CAPÍTULO III. ROLES Y RESPONSABILIDADES

COLABORADORES, DOCENTES Y ESTUDIANTES

Apropiar el manual de Seguridad de la Información mediante la incorporación de buenas prácticas en el uso de la información, sistemas de información y recursos informáticos de la Universidad EAN, como una herramienta para garantizar la confidencialidad, integridad y disponibilidad de la información institucional.

PROCESOS

Gerencia de Desarrollo Humano
Velar por el cumplimiento del Reglamento Interno de Trabajo, en los casos que aplique con respecto a los lineamientos de seguridad de la información, enunciados en el presente manual.

Gerencia de Innovación y Desarrollo de TIC

- Implementar las herramientas y controles respectivos para facilitar el cumplimiento de los lineamientos de seguridad de la información, enunciados en el presente manual
- Garantizar la operación permanente de los recursos informáticos y sistemas de información. Fortalecer la cultura digital en la Universidad EAN

LÍDERES SISTEMAS DE INFORMACIÓN

Los roles, obligaciones y responsabilidades de los líderes técnicos, líderes funcionales y usuarios finales de los sistemas de información están definidos en el documento de calidad: TIC-001-D5 Roles, Obligaciones y Responsabilidades de los Líderes Técnicos, Líderes Funcionales y Usuarios.

Líder funcional:
Es el encargado de la administración e interacción con las funcionalidades del sistema de información. Es la persona que tiene la responsabilidad de asegurar y otorgar el acceso a la información que genere el proceso y que es soportada por los Sistemas de Información de la Universidad EAN que estén a su cargo. Se considera responsable de la información al Líder de Proceso o a quien éste delegue formalmente la responsabilidad.

Líder técnico:
Es el encargado de mantener tecnológicamente los recursos informáticos y sistemas de información disponibles para su uso. Se encarga de la administración técnica del software base, entornos de ejecución, programas ejecutables y servicios del sistema.

COMITÉ DE SEGURIDAD DE LA INFORMACIÓN Y GESTIÓN DOCUMENTAL

Propender por la apropiación del Manual de Seguridad de la Información mediante la incorporación de buenas prácticas en el uso de la información, sistemas de información y recursos informáticos de la Universidad EAN, como una herramienta para garantizar la confidencialidad, integridad y disponibilidad de la información institucional. (Ver Resolución No 059 de Julio de 2012)

RESPONSABILIDADES PARA COLABORADORES

- El colaborador debe manejar de manera confidencial la información de LA UNIVERSIDAD que conozca por causa o con ocasión del ejercicio de sus obligaciones y las cuales constituyan información privilegiada, secreta, confidencial, estratégica Know How, y toda información que habiéndole sido entregada le sea indicado que no puede ser divulgada de manera que el colaborador solo podrá darle el uso adecuado o el que le haya sido autorizado en las condiciones y restricciones impartidas.
- Uno de los objetivos en la protección de la información es que no sea publicada de forma no autorizada, las instalaciones de la universidad frecuentemente son visitadas por estudiantes, proveedores, invitados, personal de aseo o terceros no autorizados, por lo tanto, se deben mantener los puestos de trabajo o escritorios limpios y organizados para evitar acceso por personal no autorizado a información de la Universidad.
- Se debe mantener el escritorio del computador, sin documentos, carpetas y/o accesos directos a información confidencial o sensible.

DISPOSICIONES

Las disposiciones aquí enmarcadas, entrarán en vigor a partir del día de su difusión.

Este manual puede ser modificado cuando el Comité de Seguridad de la Información y Gestión Documental y/o la Gerencia de Innovación de Desarrollo de TIC de la Universidad EAN lo consideren necesario, cumpliendo con el procedimiento establecido en el proceso de calidad para este tipo de documentos.

Los proveedores o terceros al igual que la comunidad EANista tienen derecho a solicitar en cualquier momento una copia de este manual vigente, así mismo tiene derecho a ejercer sus derechos como titulares de datos personales conforme a la ley vigente y aplicable.

CAPÍTULO IV. DEFINICIONES

- **Acceso autorizado**: Autorización concedida a un usuario para el uso de determinados recursos. En dispositivos automatizados es el resultado de una autentificación correcta, generalmente mediante el ingreso de usuario y contraseña.
- **Antivirus**: Son programas cuyo objetivo es detectar y/o eliminar virus informáticos.
- **Ataques de denegación de Servicio**: Es un ataque a un sistema de cómputo o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima. [2]
- **Ataques de fuerza bruta**: Intentar en repetidas ocasiones todas las posibles combinaciones de contraseñas y llaves de encriptación hasta que se encuentre la correcta.
- **Autenticación:** Procedimiento de verificación de la identidad de un usuario.
- **CD/DVD**: Dispositivo de almacenamiento de información.
- **Colaborador:** Persona que tiene vigente un contrato laboral con la Universidad EAN.
- **Conexión remota**: El uso de tecnologías de conectividad a través de una red de comunicaciones que permiten acceder e interactuar desde sitios externos al campus universitario con la infraestructura de hardware, software y servicios tecnológicos de la Universidad EAN.
- **Confidencialidad**: Protección de información privada o sensible contra divulgación no autorizada.
- **Contraseña**: Seña secreta que permite el acceso a dispositivos, información, bases de datos, recursos o servicios tecnológicos.
- **Control de acceso**: conjunto de reglas, procedimientos, prácticas, o mecanismos que permiten el ingreso a dispositivos, lugar, información o bases de datos mediante la autenticación (físico o lógico).
- **Copia de respaldo:** Copia de información en un soporte que permita su recuperación.
- **Correo vitalicio**: Cuenta de correo electrónico la cual no caduca y perdura en el tiempo.
- **Credenciales de acceso**: Datos relacionados con el usuario y contraseña para acceder a un servicio de tecnología.
- **Cuentas de proveedores que prestan servicios tecnológicos**: Son cuentas de usuario que tienen privilegios de acceso especiales con el fin de dar soporte para el mantenimiento, instalación, actualización a los recursos informáticos y sistemas de información.
- **Cuentas de usuario de Procesos**: Son cuentas de usuario que tienen privilegios de acceso especiales, generalmente como los del administrador del sistema, tienen la finalidad de ejecutar en un tiempo determinado actividades programadas para realizar modificaciones en cualquier sistema.
- **Cuentas Normales**: Cuentas nombradas que tienen todos los colaboradores, docentes, estudiantes, para acceder a los diferentes recursos informáticos y sistemas de información de la universidad.
- **Cuentas Privilegiadas**: Cuentas de administración las cuales solo tienen acceso directo ciertas personas autorizadas para labores propias de las plataformas tecnológicas, las cuales, por ser privilegiadas, están sujetas a confidencialidad. De darse a conocer podría ser utilizada con el fin de obtener un acceso no autorizado o uso indebido de los recursos de la universidad. Se utilizan para integración de aplicativos, instalación de sistemas operativos, configuración de bases de datos, administración de servidores de aplicación, ingreso a Recursos informáticos, o equipos de comunicaciones.
- **Dirección IP**: es el número con el cual se identifica un equipo de cómputo.
- **Discos de almacenamiento externo**: Los discos de almacenamiento externo son para almacenar información de forma masiva y se puede intercambiar con otros equipos.

- **Disponibilidad**: Garantizar que los sistemas de información y los datos estén listos para su uso cuando se necesite.
- **Dispositivos de almacenamiento local**: Son los discos locales del equipo de cómputo asignado para guardar cualquier tipo de información.
- **DNS**: Sistema de nombre de dominio es un sistema de nomenclatura jerárquica para equipos de cómputo, servicios o cualquier recurso conectado a Internet o a una red privada.
- **Emergencia**: Asunto o situación imprevista que requiere una especial atención y deben solucionarse lo antes posible ya que puede presentar un riesgo inmediato.
- **Equipo de cómputo**: Entiéndase como las computadoras, equipos de uso personal bien sea de escritorio o portátil y sus periféricos (Pantalla, mouse, teclado, parlantes, entre otros).
- **Gestión documental:** Es una plataforma que permite gestionar de manera ágil, segura, flexible y escalable la información institucional, tanto física como digital.
- **Hardware**: Corresponde a todas las partes físicas y tangibles de un sistema de cómputo.
- **Identificación:** Proceso de reconocimiento de la identidad de los usuarios.
- **Identificación única de usuario**: Son los datos de Usuario y contraseña de acceso a los recursos informáticos o sistemas de información.
- **Incidencia:** Cualquier anomalía que afecte o pueda afectar a la seguridad de los datos, dispositivos, equipos de cómputo, constituyendo un riesgo para la confidencialidad, disponibilidad o integridad de las bases de datos, información o servicios.
- **Incidente de Seguridad**: Es la ocurrencia de un evento o una serie de eventos, inesperados o no deseados que indican una violación, amenaza a las políticas de seguridad informática, eventos que tienden a poner en riesgo los procesos y la continuidad del negocio, así como, comprometer la confidencialidad, integridad y disponibilidad de la información de la Universidad EAN.
- **Información sensible**: información privada o confidencial de la universidad que al ser divulgada puede causar algún daño o perjuicio a la institución y sus Stakeholders.
- **Infraestructura Tecnológica**: Conjunto de recursos de telecomunicaciones, hardware y software que permitan el procesamiento, la transmisión y el almacenamiento de cualquier tipo de información.
- **Ingeniería social**: Es la práctica de obtener información confidencial a través de la manipulación de usuarios. Es una técnica que pueden usar ciertas personas, tales como investigadores privados, o personal de dudosa reputación, para obtener información, acceso o privilegios en sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riegos o abusos.
- **Integridad**: Garantiza que la información no haya sido alterada o modificada por terceros para conservar la validez de la información.
- **Licencia de software**: Permiso legal otorgado por un tercero con facultades para ello, para utilizar un programa para computador (Software) a cambio de un pago único o periódico.
- **Líder funcional**: Es el encargado de la administración e interacción con el sistema de información. Es la persona que tiene la responsabilidad de asegurar y otorgar el acceso a la información que genere el proceso y que es soportada por los Sistemas de Información de la Universidad EAN. Se considera responsable de la información al Líder de Proceso o a quien éste delegue formalmente la responsabilidad.
- **Líder técnico:** Es el encargado de mantener tecnológicamente los recursos informáticos y sistemas de información disponibles para su uso.
- **Listas externas**: Son listas externas cualquier agrupamiento de correos electrónicos diferentes a los provistos por la Universidad EAN, es decir, cuentas que estén bajo un dominio diferente a "@ean.edu.co","@universidadean.edu.co".

- **Listas externas personales**: Son aquellos agrupamientos de correos electrónicos que son creados directamente por cada usuario en su cuenta de correo para el envío de información institucional a otros servidores externos, tales como Yahoo, Hotmail, Gmail, entre otros.
- **Listas internas institucionales**: Se define como lista interna institucional, cualquier agrupamiento de cuentas de correo que se encuentren registradas y habilitadas en los servidores de correo académico y/o administrativo de la Universidad
- **Listas internas personales**: Son aquellos agrupamientos de correos que son creados directamente por cada usuario en su cuenta de correo para el envío de información a los demás usuarios internos.
- **Material de soporte:** Material en cuya superficie se registra información o sobre el cual se pueden guardar o recuperar datos, como el papel, la cinta de video, el CD, el DVD, el disco duro, etc.
- **Perfil de usuario:** Grupo de usuarios a los que se da acceso.
- **Periférico**: Elemento electrónico de entrada y/o salida de información, que pueden ser conectados a un equipo de cómputo. Son periféricos: impresoras, scanner, webcams, proyectores, pizarrones interactivos, plotters y artículos similares.
- **Programa malicioso**: Es un tipo de software que tiene como objetivo infiltrarse o dañar un equipo de cómputo, sin el consentimiento de su propietario.
- **Recurso Informático**: Son los equipos de cómputo, servidores, infraestructura tecnológica, equipos de comunicaciones, licencia de software, periférico, software, salas de cómputo, sistema de archivos, software antivirus.
- **Recurso Protegido:** Cualquier componente del sistema de información, como bases de datos, programas, soportes o equipos, empleados para el almacenamiento y tratamiento de datos personales.
- **Red Institucional**: La red institucional es la red de datos de la universidad EAN que permite la comunicación entre todos los recursos informáticos.
- **Redes Privadas Virtuales (VPN):** Una red privada virtual o VPN (siglas en inglés de Virtual Private Network), es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.
- **Responsable de seguridad:** Una o varias personas designadas por el responsable del tratamiento para el control y la coordinación de las medidas de seguridad.
- **Salas de cómputo**: Aulas acondicionadas para la disposición de una gran cantidad de equipos de cómputo.
- **Salvaguardar**: Defender, proteger un activo, información, o sistema de información
- **Seguridad de la información**: Es la protección de los activos de información, frente a una gran variedad de amenazas que existen en el mundo, con el fin de asegurar la disponibilidad de todos los procesos, minimizar el riesgo y apoyar en el cumplimiento de los objetivos de la Universidad EAN con el uso y buenas prácticas de las Tecnologías de Información y comunicación TIC.
- **Sesión de Red**: Una sesión es la duración de una conexión empleando una capa de sesión de un protocolo de red, o la duración de una conexión entre un usuario y el equipo de cómputo.
- **Servidor**: Equipo de cómputo con características que le permiten tener mayor capacidad de procesamiento que un equipo de uso personal.
- **Servidor de dominio:** Es un servidor que permite centralizar el trabajo de los usuarios de la red, sus archivos, configuraciones y perfiles, en un solo ordenador, y permite el acceso a ellos desde cualquier ordenador de la red de forma segura.
- **Sistema de archivos**: Estructura que se le asigna a un dispositivo de almacenamiento de información para la disposición de los archivos.
- **Sistema de información**: Son los sistemas, bases de datos, o aplicación de software que son administrados y que sirven de apoyo para los diferentes procesos como Sistema académico, Sistema

de nómina y recurso humano, sistema de aulas virtuales, sistema financiero entre otros y también para el tratamiento de datos personales.

- **Software**: Conjunto de componentes o instrucciones lógicas que puede ejecutar una computadora.
- **Software antivirus**: Software especializado en la detección, reconocimiento y limpieza de código malintencionado en archivos digitales.
- **Software malicioso**: Es un tipo de software que tiene como objetivo infiltrarse o dañar un equipo de cómputo sin el consentimiento de su propietario.
- **Stakeholders:** son las partes interesadas en algún proceso donde, dichas partes pueden ser personas u organizaciones, para el caso puntal de la institución es la comunidad EANista.
- **Suplantación Web**: Uso de técnicas de suplantación de sitios de Internet generalmente con usos maliciosos.
- **Teletrabajador:** Persona que desempeña actividades laborales a través de tecnologías de la información y comunicación por fuera de la Universidad. La modalidad de Teletrabajo en la Universidad EAN está orientada a los colaboradores de rol docente y administrativo que en desarrollo de sus actividades no requieran presencia en las instalaciones de la Universidad para atención a clientes o proveedores, y cumplen funciones que no requieren de aprobación inmediata o de contacto directo con sus clientes en forma presencial.
- **TIC**: Sigla para referir Tecnologías de Información y Comunicación.
- **Unidad de red o carpeta compartida**: Medios informáticos conectados en una red corporativa, para compartir y almacenar información.
- **USB**: Es un dispositivo de almacenamiento de información que utiliza una memoria flash para guardar información.
- **Usuario:** Sujeto autorizado para acceder a los datos o recursos, o proceso que accede a los datos o recursos sin identificación de un sujeto.
- **Usuario funcional:** es el profesional que opera el sistema.
- **Ventanas emergentes**: El término denomina a las ventanas del navegador de Internet que emergen automáticamente (generalmente sin que el usuario lo solicite). A menudo, las ventanas emergentes se utilizan con el objeto de mostrar un aviso publicitario de manera intrusiva.
- **Virus informático**: Es un programa que tiene por objeto alterar el normal funcionamiento de un equipo de cómputo sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de éste. Los virus pueden destruir, de manera intencionada, los datos almacenados en un sistema de cómputo.

BIBLIOGRAFÍA

- ISO. Disponibilidad. Bogotá: [citado 30 abril, 2014]. Disponible en Internet <URL:http://www.iso27000.es/glosario.html#section10c>
- INTECO. Instituto Nacional. Bogotá: [citado 30 abril, 2014]. Disponible en Internet < URL : http://www.inteco.es >
- NIST. Seguridad informática. Bogotá: [citado 30 abril, 2014]. Disponible en Internet < URL : http://csrc.nist.gov/publications/PubsSPs.html>
- ISACA. CISM. Bogotá: [citado 30 abril, 2014]. Disponible en Internet < URL : https:// www.isaca.org/Pages/default.aspx >
- Manual interno de Seguridad. Realizado por Certicamara para la Universidad EAN. Febrero de 2016.