FIRMA DIGITAL
Firmado digitalmente por: MAURICIO GIRON Jose Alberto FAU 20131367938 soft
Motivo: Soy el autor del documento
Fecha: 09/09/2022 13:40:41-0500

INTRODUCCIÓN

La Escuela Superior Conjunta de las Fuerzas Armadas (ESCOFFAA) es una institución educativa de Educación Superior que tiene como objetivo fomentar la capacitación, especialización y perfeccionamiento en materias conjuntas, en las áreas de Desarrollo, Seguridad y Defensa Nacional.

De otro lado, la Ley 29733, Ley de Protección de Datos Personales, y su reglamento nos obliga a cuidar y no develar información de carácter privado de las personas con las que ESCOFFAA interactúa, así como de obtener la autorización expresa de cada base de datos que ESCOFFAA pudiese tener.

La seguridad de la información preserva la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión del riesgo y garantiza, a las partes interesas, que los riesgos sean administrados adecuadamente. La seguridad de la información se define como la salvaguarda de la información para:

- Su confidencialidad, asegurando que sólo quienes estén autorizados puedan acceder a la información;
- Su integridad, asegurando que la información y sus métodos de proceso sean exactos y completos; y
- Su disponibilidad, asegurando que los usuarios autorizados tengan acceso a la información cuando la requieran.

1. OBJETIVO

Esta política tiene como objetivo establecer los lineamientos para la gestión de la seguridad de la información, así como para la implementación de medidas con la finalidad de preservar la confidencialidad, integridad y disponibilidad de los activos de información de la ESCOFFAA.

2. ALCANCE

Esta política es aplicable a:

- Servidores / funcionarios de la ESCOFFAA, independientemente de su condición contractual, de sus funciones, y de su nivel jerárquico.
- Docentes.
- Alumnos.
- Directores.
- Proveedores.
- Terceros que actúen en nombre de ESCOFFAA.

Firmado digitalmente por: MAURICIO GIRON Jose Alberto FAU 20131367938 soft
Motivo: Soy el autor del documento
Fecha: 09/09/2022 13:41:10-0500
FIRMA DIGITAL

3. DEFINICIONES

- **Activo de información**: Información o soporte en que ella reside, que es gestionado de acuerdo con las necesidades de la ESCOFFAA y los requerimientos legales, de manera que puede ser entendida, compartida y usada. Es de valor para la organización y tiene un ciclo de vida.
- **Amenaza**: Evento que puede afectar adversamente la operación de la ESCOFFAA y sus activos de información, mediante el aprovechamiento de una vulnerabilidad.
- **Autenticación**: Es el proceso que permite verificar que una entidad es quien dice ser, para lo cual hace uso de las credenciales que se le asignan. La autenticación puede usar uno, dos o más factores de autenticación independientes, de modo que el uso sin autorización de uno de ellos no compromete la fiabilidad o el acceso a los otros factores.
- **Base de datos personales**. Conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso.
- **Base de datos personales de administración privada**. Banco de datos personales cuya titularidad corresponde a una persona natural o a una persona jurídica de derecho privado, en cuanto el banco no se encuentre estrictamente vinculado al ejercicio de potestades de derecho público.
- **Base de datos personales de administración pública**. Banco de datos personales cuya titularidad corresponde a una entidad pública.
- **Ciberseguridad:** Protección de los activos de información mediante la prevención, detección, respuesta y recuperación ante incidentes que afecten su disponibilidad, confidencialidad o integridad en el ciberespacio; el que consiste a su vez en un sistema complejo que no tiene existencia física, en el que interactúan personas, dispositivos y sistemas informáticos.
- **Credencial:** Conjunto de datos que es generado y asignado a una entidad o un usuario para fines de autenticación.
- **Datos personales.** Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados.
- **Datos sensibles.** Datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos; opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual.
- **Encargado de tratamiento de datos personales.** Es la persona encargada de alimentar, almacenar, cuidar los datos personales que maneja la ESCOFFAA; así como asegurarse de tener la autorización de dicha base de datos.
- **Entidad:** Usuario, dispositivo o sistema informático que tiene una identidad en un sistema, lo cual la hace separada y distinta de cualquier otra en dicho sistema.

FIRMA DIGITAL
Firmado digitalmente por: MAURICIO GIRON Jose Alberto FAU 20131367938 soft
Motivo: Soy el autor del documento
Fecha: 09/09/2022 13:41:22-0500

- **Evento:** Un suceso o serie de sucesos que puede ser interno o externo a la organización originada por la misma causa, que ocurre durante el mismo periodo de tiempo.
- **Factores de autenticación de usuario:** Aquellos factores empleados para verificar la identidad de un usuario, que pueden corresponder a las siguientes categorías:
  - Algo que solo el usuario conoce.
  - Algo que solo el usuario posee.
  - Algo que el usuario es, que incluye las características biométricas.
- **Incidente**: Evento que se ha determinado que tiene un impacto adverso sobre la organización y que requiere de acciones de respuesta y recuperación.
- **Información:** Datos que pueden ser procesados, distribuidos, almacenados y representados en cualquier medio electrónico, digital, óptico, magnético, impreso u otros, que son el elemento fundamental de los activos de información.
- **Servicios en nube:** Servicio de procesamiento de datos provisto mediante una infraestructura tecnológica que permite el acceso de red a conveniencia y bajo demanda, a un conjunto compartido de recursos informáticos configurables que se pueden habilitar y suministrar rápidamente, con mínimo esfuerzo de gestión o interacción con los proveedores de servicios.
- **Procesamiento de datos:** El conjunto de procesos que consiste en la recolección, registro, organización, estructuración, almacenamiento, adaptación, recuperación, consulta, uso, transferencia, difusión, borrado o destrucción de datos.
- **Titular de datos personales.** Persona natural a quien corresponde los datos personales.
- **Titular del banco de datos personales.** Persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad.
- **Transferencia de datos personales.** Toda transmisión, suministro o manifestación de datos personales, de carácter nacional o internacional, a una persona jurídica de derecho privado, a una entidad pública o a una persona natural distinta del titular de datos personales.
- **Tratamiento de datos personales**. Cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales.
- **Usuario:** persona natural o jurídica que utiliza o puede utilizar los productos ofrecidos por la ESCOFFAA.

FIRMA DIGITAL
Firmado digitalmente por: MAURICIO GIRON Jose Alberto FAU 20131367938 soft
Motivo: Soy el autor del documento
Fecha: 09/09/2022 13:41:34-0500

- **Vulnerabilidad:** Debilidad que expone a los activos de información ante amenazas que pueden originar incidentes con afectación a los mismos activos de información, y a otros de los que forma parte o con los que interactúa.

4. LINEAMIENTOS

- La política es comunicada, entendida e implementada en toda la organización y es de conocimiento de todos miembros de la ESCOFFAA: SERVIDOR/FUNCIONARIO, funcionarios, directores, proveedores, y demás grupos de interés pertinentes.
- Todos los servicios de tecnología de la información se encuentran sujetos a monitoreo y en caso de detectarse un mal uso de los recursos se aplicarán las medidas correctivas.
- Todos los usuarios deben notificar los incidentes de seguridad de la información conforme a los canales de comunicación establecidos.
- Reportar inmediatamente los eventos que atenten contra la seguridad de la información a través de los canales establecidos al responsable de integridad y/o a la Dirección General.

4.1 Tratamiento de los datos. La información que está en las bases de datos de la ESCOFFAA es sometida a distintas formas de tratamiento, como recolección, intercambio, actualización procesamiento, reproducción, compilación, almacenamiento, uso, sistematización y organización, todos ellos de forma parcial o total en cumplimiento de las finalidades aquí establecidas. La información podrá ser entregada, transmitida o transferida a entidades públicas. En todo caso, la entrega, transmisión o transferencia se hará previa suscripción de los compromisos que sean necesarios para salvaguardar la confidencialidad de la información. La información personal, incluyendo información sensible, podrá ser transferida, transmitida o entregada a otra institución, independientemente del nivel de seguridad de las normas que regulen el manejo de información personal.

4.2 Recursos. La ESCOFFAA asegura la disponibilidad de recursos necesarios para la gestión de la seguridad de la información y protección de datos personales.

- En los puestos de trabajo, computadoras portátiles o Smartphones proporcionados por la ESCOFFAA, se puede instalar únicamente las aplicaciones permitidas por lo que queda prohibido el uso de software no autorizado.
- La oficina de Tecnología de la Información y Comunicaciones en coordinación con el equipo de soporte técnico planifica anualmente las actividades de capacitación y concienciación en Seguridad de la Información para todos los señalados en el alcance de la presente política.

Firmado digitalmente por: MAURICIO GIRON Jose Alberto FAU 20131367938 soft
Motivo: Soy el autor del documento
Fecha: 09/09/2022 13:41:47-0500
FIRMA DIGITAL

4.3 Proveedores.

- Los mecanismos de control con proveedores aseguran que estos cumplan con la política de seguridad de la información establecida por la organización.
- Todo cambio en los servicios que preste un proveedor es comunicado, acordado y planificado antes de realizarse.

4.4 Uso de redes.

- Cada usuario es responsable de todas las actividades que realiza con sus cuentas de usuario del dominio, correo electrónico institucional y sistemas de información asociados a la ESCOFFAA.
- El uso de la red interna, correo electrónico institucional, internet, computadoras de escritorio y portátiles e impresoras son para fines estrictamente laborales.
- Queda terminantemente prohibido utilizar el internet para descargar archivos de ocio, entrar a redes sociales, blog, radio y televisión en línea, videos en línea, juegos, chat a excepción de que sean obligaciones laborales y/o autorizadas.
- Queda terminantemente prohibido utilizar internet para ver contenido pornográfico, descargar cualquier tipo de software sin autorización y piratería informática, así como para la evasión del equipo de seguridad perimetral (firewall).
- Está prohibido enviar mensajes de correo electrónico que contengan datos de carácter personal o de terceros que puedan vulnerar la seguridad de estos.
- Los archivos adjuntos a un correo electrónico deben ser menores o iguales a 20MB.
- Cuando un archivo excede la capacidad máxima de 20 MB existen niveles de seguridad en el uso y habilitación de un Drive en nube donde se pueden compartir archivos de mayor tamaño manteniendo la confidencialidad de la información.
- Cuando un emisor de un correo electrónico sea desconocido no se debe abrir dicho correo ni descargar ningún documento adjunto. En este punto solicitar siempre el apoyo del área de TIC.

4.5 Clasificación de la información. Se ha establecido una clasificación para la información la misma que puede ser tratada como confidencial, interna o pública, conforme lo señalado a continuación:

a) Confidencial: La ESCOFFAA considera como información confidencial aquella información de carácter no público, referida a lo siguiente:

- Documentos de instrucción que se detallan la realización de Ejercicios Conjuntos.
- Fechas de cumpleaños del personal ESCOFFAA.

Firmado digitalmente por: MAURICIO GIRON Jose Alberto FAU 20131367938 soft
Motivo: Soy el autor del documento
Fecha: 09/09/2022 13:42:02-0500
FIRMA DIGITAL

- Nombres de las señoras madres o esposas del personal ESCOFFAA.
- Videos editados de cátedras con material sensible, usuarios alumnos del PCEMC en el Aula Virtual.

A fin de preservar la reserva de esta información, los usuarios de la ESCOFFAA deberán firmar el Anexo 1 *"Compromiso de Confidencialidad y Tratamiento de Datos Personales"*; por lo que la violación a estos compromisos podrá generar acciones disciplinarias, establecidas de acuerdo con normativas internas y de protección de datos.

b) Interna: Es la información que genera, utiliza y controla la organización continuamente. Las atribuciones de generación, modificación y eliminación están limitadas de acuerdo con las funciones o roles de cada usuario. Este tipo de información también puede ser compartida con las partes interesadas según lo crea conveniente la organización. Por ello, cada usuario tiene la responsabilidad de custodiar la seguridad de la información concedida en cualquier medio de soporte (digital o físico).

- Plan de Mantenimiento de soporte informático.
- Documentación diaria de coordinación entre las oficinas y departamentos de la ESCOFFAA.
- Notas de los alumnos de los Programas Académicos.
- Relación del Personal que participó en los Programas Académicos.
- Tramitación para los pagos de los docentes.
- Relación de los docentes.
- Sílabos.
- Planes.
- Programas curriculares.
- Programas educativos.
- Resultados de las evaluaciones.
- Procedimientos internos.
- Bases de datos.
- Resoluciones Directorales.
- Documentos del Consejo Académico.
- Proceso de selección de docentes para los programas académicos.
- Papeletas de permiso.
- Información de contacto con los integrantes de los comités de la revista (correos electrónicos, números telefónicos).

Firmado digitalmente por: MAURICIO GIRON Jose Alberto FAU 20131367938 soft
Motivo: Soy el autor del documento
Fecha: 09/09/2022 13:42:16-0500
FIRMA DIGITAL

- Información de contacto con los articulistas de la revista (correos electrónicos, números telefónicos).
- Información de contacto con los agregados castrenses acreditados en el Perú (correos electrónicos, números telefónicos).
- Nombres de los revisores asignados a los artículos presentados a la revista Pensamiento Conjunto.
- Videos editados de ceremonias, cátedras y conferencias para usuarios del Aula Virtual.
- Directivas web, revista, privacidad de datos para la web de la revista en línea, ceremonia, efemérides, plan anual de comunicación social. • Cartas, oficios, invitaciones a CCFFAA, IIAA, PNP, agregados castrenses acreditados en el Perú, integrantes de los comités de la revista Pensamiento Conjunto y articulistas.
- Oficios de comunicación interna a las diversas áreas responsables de brindar información

c) Pública: Es la información que la ESCOFFAA ha establecido que puede ser compartida, de acuerdo con la Política de Transparencia y Divulgación de la Información, y la que estará disponible en la web de la ESCOFFAA; esta información está relacionada a las contrataciones que mantiene con el Estado, siendo estas de carácter público, según lo establecido por la norma de transparencia de la información.

- Misión y Visión, organigrama, valores, objetivos, historia y heráldica ESCOFFAA.
- Resoluciones directorales, políticas institucionales, convocatorias de selección de docentes.
- Hojas de vida/fotos de directores de la ESCOFFAA, docentes facilitadores y docentes contratados por horas.
- Competencias y perfiles de ingreso y egreso de los programas académicos.
- Objetivos, competencias, perfiles de ingreso y egreso, programación curricular y duración de los programas virtuales.
- Libros en pdf editados por la ESCOFFAA • Ediciones de la revista Pensamiento Conjunto.
- Trabajos de investigación PCEMC aprobados para su publicación.
- Noticias y fotografías de eventos ESCOFFAA.
- Relación nominal de los primeros puestos PCEMC. • Relación nominal de las promociones PCEMC.
- Glosario militar conjunto.

Firmado digitalmente por: MAURICIO GIRON Jose Alberto FAU 20131367938 soft
Motivo: Soy el autor del documento
Fecha: 09/09/2022 13:42:30-0500
FIRMA DIGITAL

- Relación de efemérides.

4.6 Uso de la información

- Toda información interna o confidencial es visualizada dentro de una red o conexión segura.
- Toda información interna o confidencial (impresa o escrita) así como la información contenida en dispositivos de almacenamiento (CD, DVD, USB) son guardadas en un lugar seguro.
- Los usuarios que, por la naturaleza de sus funciones, impriman documentos con información confidencial, la deben retirar de la impresora inmediatamente.
- Los usuarios deben mantener el escritorio de trabajo ordenado y libre de todo tipo de información interna o confidencial, para lo cual lo debe almacenar en las carpetas compartidas de área correspondiente.
- Los usuarios velan por la seguridad y confidencialidad de la información contenida en sus equipos, especialmente cuando se encuentren fuera de las dependencias de la organización.
- La entrega de listados o de Base de Datos se realiza a personas autorizadas y con la autorización de la Dirección General.
- Los usuarios no deben distribuir o eliminar registros o información importante sin la aprobación respectiva de los propietarios de información.
- Toda información en papel o contenida en dispositivos de almacenamiento que contengan información clasificada como confidencial, y se desee eliminar, es destruida de modo que sea imposible su recuperación.
- Toda información del servidor / funcionario es administrada y controlada únicamente por el personal autorizado por la Dirección General.
- Retener u ocultar información necesaria para el desarrollo de procesos internos, o para el desarrollo de las actividades propias de la ESCOFFAA, se considera una falta grave por lo que el personal y/o funcionarios que incumplan con este principio serán sancionados de acuerdo con las normativas internas.
- Si el servidor / funcionario está autorizado a compartir información confidencial, deberá aplicar el buen criterio para limitar la cantidad de información y el período por el cual será compartida; y divulgar la misma en función a la necesidad de conocimiento. Se deberá cerciorar, asimismo, de que el destinatario:
  - Conoce que la información es confidencial,
  - Ha sido instruido sobre las restricciones respecto a su posterior uso y revelación y
  - Conoce los procedimientos, así como las responsabilidades adicionales a las que se obliga por tener acceso a dicha información.

Firmado digitalmente por: MAURICIO GIRON Jose Alberto FAU 20131367938 soft
Motivo: Soy el autor del documento
Fecha: 09/09/2022 13:42:58-0500
FIRMA DIGITAL

- Uso, manipulación, custodia, almacenamiento y tratamiento de legajos personales en específico de Oficiales del Ejército Peruano, que son destacados /asignados a esta Escuela Superior Conjunta. Dicho procedimiento deberá ser coordinado con la Dirección Administrativa.
- Uso, manipulación, custodia, tratamiento, almacenamiento y tratamiento de información personal de Oficiales de Instituciones Armadas y/o participantes civiles que pudiese tener la Dirección Administrativa para efectos de control.
- Para el caso de gestión académica, deberá establecer en dicho procedimiento, que las Actas de Notas, sílabos, documentos, publicaciones, hojas previas y todo lo relacionado a la parte académica, deberá estar en la plataforma virtual durante el año fiscal, siendo retirado de la misma al término, quedando dicha información en los servidores de esta Escuela.
- El acceso a la información anteriormente descrita, será solo para personal con autorización, que cuente con usuario y contraseña debidamente asignada por la oficina de Tecnología de la Información y Comunicaciones. La información no es de carácter abierta o pública.
- El acceso a la información de gestión académica deberá ser solicitada por escrito, considerando los formatos establecidos en la plataforma virtual ya existente (constancias, certificados, diplomas). El resto de documentación, será considerada en los procedimientos de trámite documentario de esta Escuela Superior Conjunta.

4.7 Destrucción de documentos impresos

- La ESCOFFAA, deberá dar cumplimiento a las normas y disposiciones estipuladas en la Ley N° 24444 (Ley del Procedimiento Administrativo General), RM N° 392-2011-DE/SEG 28 ABR 2011, Directiva General N° 008-2011 MD/SG-UAIP Abr 2011 (procedimientos para el acceso, clasificación, reclasificación, desclasificación, archivo y conservación de la información del Sector Defensa.
- Los documentos administrativos de los archivos de las entidades del Sector Defensa, cuya conservación sea innecesaria podrán ser eliminados o incinerados previa acta de incineración y/o destrucción.
- Se deberá emplear al máximo el triturador de papeles, ubicado en la oficina de mesa de partes, para la destrucción de los borradores de trabajo.
- El personal debe dar estricto cumplimiento al control, supervisión y verificación física de la destrucción total de los borradores de trabajo a fin de evitar la fuga de información.
- El Oficial de Seguridad, realizará la verificación y constatación del cumplimiento estricto del procedimiento de destrucción de documentos (borradores), mediante inspecciones inopinadas.

Firmado digitalmente por: MAURICIO GIRON Jose Alberto FAU 20131367938 soft
Motivo: Soy el autor del documento
Fecha: 09/09/2022 13:43:13-0500
FIRMA DIGITAL

4.8 Intercambio de información y correo electrónico. Los mensajes de correo electrónico deben ser considerados de igual manera que un memorándum formal, son considerados como parte de los registros de la ESCOFFAA y están sujetos a monitoreo y auditoria.

Los sistemas de correo electrónico no deben ser utilizados para lo siguiente:

- Enviar cadenas de mensajes.
- Enviar mensajes relacionados a seguridad, exceptuando al personal encargado de la administración de la seguridad de la información.
- Enviar propaganda de candidatos políticos.
- Actividades ilegales, no éticas o impropias.
- Actividades no relacionadas al quehacer de la ESCOFFAA.
- Diseminar direcciones de correo electrónico a listas públicas.
- Para acceder al correo electrónico se facilitará una dirección electrónica y una contraseña inicial que deberá ser cambiada inmediatamente una vez recibida para mantener la confidencialidad de esta. Las personas usuarias tomarán todas las medidas oportunas para mantener su carácter confidencial.
- Cualquier solicitud posterior de correo de cambio de contraseña dirigida a los administradores del servicio deberá realizarse previa identificación del titular de la cuenta y sólo al titular se le podrá facilitar dicha contraseña.
- Si algún miembro de la ESCOFFAA que por razones del servicio o por que dejó de laborar algún SERVIDOR/FUNCIONARIO, desea tener acceso a la contraseña del mencionado SERVIDOR/FUNCIONARIO, o de una cuenta de la que no es titular se compromete a no divulgarla, mantenerla y a no eliminar información ni a hacer uso impropio de ella.
- No debe utilizarse reglas de reenvío automático de información de la ESCOFFAA a direcciones que no pertenecen a la organización. No existe control sobre los mensajes de correo electrónico una vez que estos se encuentran fuera de la red de la ESCOFFAA.
- Se establecerá un proceso formal para aprobar la publicación de información de la ESCOFFAA. El desarrollo de páginas Web debe considerarse como desarrollo de software y debe estar sujeto a los mismos controles.
- Si el usuario usa sistemas o carpetas públicas, éstas no deben contener información restringida, confidencial o de uso interno de la ESCOFFAA. Es decir, las plataformas externas que brindan servicios web, correo electrónico, comercio electrónico u otros servicios públicos (ejemplo: Gmail, Yahoo, Hotmail, Dropbox, etc. de uso personal) no deben almacenar información restringida, confidencial o de uso interno; ésta debe ser almacenada en los servidores y equipos corporativos que brinda la ESCOFFAA.

Firmado digitalmente por: MAURICIO GIRON Jose Alberto FAU 20131367938 soft
Motivo: Soy el autor del documento
Fecha: 09/09/2022 13:43:26-0500
FIRMA DIGITAL

4.9 Acceso lógico. Todos los accesos a los recursos de información están basados en la necesidad y perfil de puesto del usuario, razón por la cual se toman en cuenta los siguientes aspectos:

- Acceso basado en roles.
- Segregación de roles de control de acceso.
- Los requerimientos de seguridad de cada uno de los sistemas de información considerando siempre el principio de menor privilegio.
- Identificación de toda la información relacionada a las aplicaciones y los riesgos a la que está expuesta.
- Requisitos para la autorización formal de las solicitudes de acceso.
- Administración de derechos de acceso privilegiado
- Revisión periódica de los controles de acceso.
- Revocación de los derechos de acceso.
- Todas las estaciones de trabajo que tienen acceso a la red interna de la ESCOFFAA deben ser parte del Directorio Activo, a fin de asegurar que no comprometan la seguridad de los activos de información.
- El acceso a la red interna de la ESCOFFAA es controlado mediante políticas de seguridad aplicadas según perfiles de usuario para los servidores / funcionarios.
- Todas las estaciones de trabajo y computadoras portátiles están configuradas para bloquear automáticamente el equipo una vez transcurrido los 10 minutos de inactividad.
- Los servidores / funcionarios deben bloquear el equipo cada vez que se retiren de su puesto de trabajo de forma manual (combinación de teclas “WINDOWS” +” L”).

4.10 Uso de contraseñas

- A los servidores / funcionarios se les crea usuario y contraseña temporal de inicio de sesión para el acceso a las distintas aplicaciones internas, considerando su perfil de puesto.
- Dichas contraseñas deben ser sustituidas en su primer acceso de inicio de sesión por una contraseña compleja, según lo permita la aplicación.
- Estas son de uso personal e intransferible. Ningún usuario debe solicitar las contraseñas de otros usuarios.
- Las contraseñas de acceso al sistema y aplicaciones deben ser cambiadas con una periodicidad trimestral y deben ser distintas a las cinco últimas.
- No se utilizan las funciones de recordar las contraseñas en ninguna de las aplicaciones proporcionada o requeridas por la organización.
- Las contraseñas no se deben escribir en soportes de fácil extravío o divulgación.
- No se deben usar contraseñas de la organización para sistemas externos como correos personales y herramientas web.

Firmado digitalmente por:
MAURICIO GIRON Jose
Alberto FAU 20131367938 soft
Motivo: Soy el autor del documento
Fecha: 09/09/2022 13:43:41-0500
FIRMA DIGITAL

- Los usuarios deben tomar las precauciones para proteger su contraseña.
- En caso de no recordarla o se produzca el bloqueo de sesión, se comunicarán según los canales establecidos para restablecerla.
- Para restablecer la contraseña se validan algunos datos personales del usuario según los lineamientos establecidos en el proceso correspondiente.
- Si algún usuario sospechara que otro usuario conoce su contraseña, inmediatamente debe cambiar dicha contraseña y comunicar lo sucedido según los canales establecidos por la organización.

4.11 Protección contra software malicioso

- La organización adopta las medidas necesarias para la prevención, detección y eliminación de software malicioso a nivel de la red, servidores, estaciones de trabajo, computadoras portátiles.
- Se asegura que todos los servidores, estaciones de trabajo y computadoras portátiles de la ESCOFFAA estén protegidas con una solución contra software malicioso que tiene capacidad de actualización automática.
- Se implementan medidas de software malicioso a los sistemas de información que pertenecen a la organización.
- Se asegura que el sistema operativo y los aplicativos de las estaciones de trabajo y computadoras portátiles de la ESCOFFAA, tengan las últimas actualizaciones de seguridad con la finalidad de evitar la explotación de vulnerabilidades técnicas.
- Se implementan controles que eviten o detecten el uso de software no autorizado y controles que eviten o detecten el ingreso a sitios web que se sospecha son maliciosos.

4.12 Acceso físico

- El personal de la ESCOFFAA, docentes, alumnos y terceros que tengan acceso a las instalaciones de la Escuela, deberán registrarse con el "Servicio de Permanencia de la ESCOFFAA" a través del "CUADERNO DE CONTROL RESPECTIVO DE LA ESCOFFAA".
- Se ha establecido una clasificación de las áreas, dentro de las instalaciones de la ESCOFFAA, para definir el nivel de seguridad de estas la que se describe a continuación:

    - **Áreas Restringidas**: son zonas seguras donde la información que se genera trata o almacena es crítica para la organización (Información clasificada como confidencial). Los accesos a estas zonas son controlados. Solo tendrán acceso a ella las personas que por la naturaleza de su función deben conocerla, para tal fin deberá llenar el compromiso de confidencialidad y tratamiento de datos personales.

- **Áreas Específicas**: Son zonas seguras que sólo tiene una función específica y no podrá ser utilizada para otros fines. Los accesos a estas zonas son controlados.

- **Áreas Comunes**: son zonas de uso común para todos los usuarios de la ESCOFFAA.

- **Áreas Públicas**: Son zonas que son de utilización común y de recepción de personas externas a la organización.

- La ESCOFFAA, ha definido un mapa de instalaciones en el cual se indica el nivel de seguridad de cada área y se clasifican las áreas físicas determinando el nivel de seguridad de estas.
- Las áreas de carga y descarga están determinadas y señaladas en el mapa de instalaciones como zona pública (zona de parqueo de vehículos de la instalación).
- El Servicio de Permanencia de la ESCOFFAA, controla el acceso de personas ajenas a la instalación (incluyendo proveedores u otros), se asegura que los datos del visitante sean anotados en el “CUADERNO DE CONTROL DE VISITAS DE LA ESCOFFAA”.
- Todo visitante que se encuentre dentro de a las instalaciones debe portar en todo momento su pase de visita otorgado por el Servicio de Permanencia de la ESCOFFAA, de manera obligatorio mientras permanezca dentro de las instalaciones.
- Toda persona ajena a la instalación podrá acceder a las áreas definidas como restringidas o específicas, siempre que cuente con la autorización correspondiente y están siempre acompañado por personal de la oficina de seguridad.
- Los alumnos de los diferentes programas académicos no podrán transitar por el área del departamento de evaluación.
- Se debe contar con autorización de la dirección de la ESCOFFAA, para el retiro de equipos de información o software de propiedad.
- Las medidas de protección contra amenazas externas y ambientales se encuentran definidas en el Plan de Seguridad de la instalación, incluyen:
- Controles de acceso y seguridad física.
  - Plan contraincendios.
  - Plan de Evacuación.
  - Croquis de distribución de extintores.
  - Sistema de Video vigilancia (CCTV).

4.13 Soporte informático

- Los usuarios la ESCOFFAA son responsables de mantener operativos los equipos asignados a su cargo.
- Los usuarios de la ESCOFFAA toman todas las precauciones necesarias para evitar la pérdida o daño del equipo.
- Cuando los usuarios abandonen la oficina en la que laboran, deben apagar su computadora.
- Se realiza mantenimiento a los equipos informáticos conforme al "**PLAN DE MANTENIMIENTO Y RENOVACIÓN DE EQUIPOS TECNOLÓGICOS DE LA ESCOFFAA**" y el registro de estas.
- Cuando el usuario deja de laborar o mantener una relación contractual con la ESCOFFAA, deberá devolver todos los equipos y dispositivos asignados a su cargo.
- Antes de que se reasignen o se den de baja a las computadoras, se asegura que la información ubicada en los discos duros de estos haya sido eliminada o sobrescrita de manera segura de modo que su recuperación sea irreversible.
- Se recomienda a los usuarios no consumir alimentos en los puestos de trabajo ya que pueden originar deterioro de los equipos y de la documentación de la Escuela.

4.14 Gestión de riesgos

- Se identifican, cuantifican y priorizan los riesgos de seguridad de la información utilizando la metodología adoptada a fin de poder establecer los controles apropiados para el tratamiento de cada uno de los riesgos identificados.
- La evaluación de riesgos se realiza cada vez que se identifiquen cambios significativos dentro de la institución y en el caso de que no se presente dicha situación, la evaluación se realiza como mínimo una vez al año.
- Los métodos utilizados en la gestión de proyectos de la organización integran los controles de seguridad de la información para asegurarse que se identifican y tratan los riesgos de seguridad de la información.

4.15 Respaldo y recuperación de la información.

- Las copias de seguridad de la información (BACKUP) de la ESCOFFAA son realizadas, registradas y controladas periódicamente. Estas copias de seguridad se realizan considerando la criticidad de información.
- La frecuencia de las copias de seguridad se realizará en base a la importancia y sensibilidad de la información almacenada.
- Los ambientes donde se almacenen o resguarden las copias de seguridad cumplen las condiciones adecuadas de acondicionamiento, temperatura y humedad.

- Se realizan pruebas de restauración a las copias de seguridad a fin de asegurar que se pueda obtener correctamente la información almacenada al momento de ser necesaria.
- Los equipos de respaldo cuentan con un programa de mantenimiento para asegurar su correcto funcionamiento.

4.16 Continuidad

- Se incluye la continuidad de la seguridad de la información dentro del proceso de Gestión de la Continuidad del Negocio.
- Se asegura la existencia de recursos para el tratamiento de la información redundante que satisfacen los requerimientos de disponibilidad del servicio.

INCUMPLIMIENTO

La falta o transgresión a la presente política constituirá una infracción grave sancionable conforme a la normativa interna vigente.

Todos los miembros de la ESCOFFAA que tomen conocimiento de alguna violación de la presente política deben denunciarlo a través de los canales de denuncia establecidos.

Toda la información es retenida conforme a los requisitos legales.

- Se establecen los términos, condiciones y finalidades para datos personales en cumplimiento con la ley existente y su reglamento.
- Se cumple con las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos, y de los requisitos legales de seguridad.
- Los servidores / funcionarios de la ESCOFFAA mantienen la confidencialidad sobre toda la información y datos de carácter personal y de terceros a los que tengan acceso en virtud de su trabajo, obligación que subsistirá incluso hasta 3 años después de finalizar su relación con la organización.

ANEXO 1- COMPROMISO DE CONFIDENCIALIDAD Y TRATAMIENTO DE DATOS PERSONALES

Conste en el presente documento privado, el compromiso de confidencialidad por parte del Sr(a).

_____, con DNI/CE N° _____, con domicilio en _____ y con el cargo de _____ quien en adelante se le denominará EL SERVIDOR/FUNCIONARIO; y por la otra parte, la ESCOFFAA identificado con número de RUC N° _____ , y con domicilio fiscal en _____ en adelante EL EMPLEADOR, han acordado lo siguiente:

1. EL SERVIDOR/FUNCIONARIO se obliga a conocer los alcances de la Ley N° 29733 Ley de Protección de Datos Personales, y los alcances de la Política de Seguridad de la Información y Protección de Datos de la ESCOFFAA, sus prohibiciones y lineamientos.
2. EL SERVIDOR/FUNCIONARIO se compromete a respetar y aplicar en la ejecución de las funciones designadas, las políticas, procedimientos, estándares y controles de seguridad de la información establecidos por EL EMPLEADOR.
3. EL SERVIDOR/FUNCIONARIO deberá proteger la información[1] de EL EMPLEADOR, comprometiéndose a no incurrir e informar acerca de eventos relacionados con el acceso no autorizado, pérdida, modificación y/o destrucción, falsificación, robo, uso indebido, divulgación u algún otra eventualidad que comprometa la integridad, disponibilidad y/o confidencialidad de la información de EL EMPLEADOR.
4. EL SERVIDOR/FUNCIONARIO deberá mantener y guardar estricta reserva, absoluta confidencialidad y no deberá difundir o entregar ni hacer pública por ningún tipo de medio la información de EL EMPLEADOR, a la que pueda acceder directa o indirectamente durante la ejecución de sus funciones en la ESCOFFAA.
5. EL SERVIDOR/FUNCIONARIO solo podrá hacer uso de la información a la cual tenga acceso por la naturaleza de sus funciones con el personal que se encuentre debidamente autorizado.

En el caso que EL SERVIDOR/FUNCIONARIO fuera requerido por alguna autoridad administrativa o judicial para revelar la información y/o documentación a la que se refiere el presente documento, EL SERVIDOR/FUNCIONARIO deberá poner este hecho en conocimiento de EL EMPLEADOR para los fines pertinentes.

EL EMPLEADOR y EL SERVIDOR/FUNCIONARIO establecen que la vigencia de las disposiciones del presente documento relacionadas a la reserva y confidencialidad de la información inicia desde la fecha de suscripción del presente documento y se mantendrá vigente incluso hasta 3 años posteriores a la extinción del vínculo laboral.

FECHA: _____

APELLIDOS Y NOMBRES DEL SERVIDOR/FUNCIONARIO: _____

DNI/CE: _____ FIRMA: _____

[1] Datos y/o información de valor para la ESCOFFAA y sus asociados y que la divulgación y/o el uso o tratamiento indebido comprometa su imagen institucional o funcionamiento, la cual se encuentre almacenada o haya sido compartido en cualquiera de sus formas (ambientes digitales, sistemas de información, dispositivos de almacenamiento, equipos de audio y video, documentos físicos, información brindada verbalmente directa o indirectamente, etc.)