Memorando Nro. MD-DTIC-2021-0114-MEM

Quito, D.M., 08 de junio de 2021

PARA: Ing. Vilma Ávila Toledo
Analista de Tecnologías de la Información 2

Srta. Ing. Andrea Stefania Valdivieso Romero
Asistente de Tecnologías de la Información-SP1

ASUNTO: Solicitud documentación de cumplimiento al grupo "No. 05 CONTROL DE ACCESO" del Esquema Gubernamental de Seguridad de la Información EGSI

ANTECEDENTES:

• Mediante Oficio Nro. SNAP-SNADP-2013-000227-O de 25 de septiembre de 2013, la Secretaria Nacional De La Administración Pública dispone al Ministerio del Deporte:
"Adjunto para su conocimiento y fines pertinentes Acuerdo No. 166 de 19 de septiembre de 2013, mediante el cual se dispone a las entidades de la Administración Pública Central, Institucional y que depende de la Función Ejecutiva el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO 27000 para la Gestión de Seguridad de la Información."

• El ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN EGSI, Acuerdo Ministerial No. 025-2019, Registro Oficial Edición Especial 228 de 10-ene.-2020, emitido por el Ministro de Telecomunicaciones y de la Sociedad de la Información señala:

5. CONTROL DE ACCESO			
5.1	Requisitos institucionales para el control de acceso		
	5.1.1	Política de control de acceso Control Elaborar, implementar y socializar la política de control de acceso a los sistemas de información, de acuerdo a la necesidad institucional y considerando la seguridad de la información. Recomendaciones para la implementación:	
		5.1.1.1	Gestionar los accesos de los usuarios a los sistemas de información asegurando el acceso de usuarios autorizados y previniendo los accesos no autorizados.
		5.1.1.2	Definir responsabilidades para identificar, gestionar y mantener perfiles de los custodios de información.
		5.1.1.3	Definir los requisitos para la autorización formal de los pedidos de acceso.
		5.1.1.4	Revisión periódica de los usuarios y los permisos otorgados, retirando aquellos permisos que hayan cambiado su situación
		5.1.1.5	Definir claramente los autorizadores de los permisos de acceso a la información,
		5.1.1.6	Relación directa entre los derechos de acceso y las políticas de clasificación de la información de sistemas y redes.
		5.1.1.7	Definir la política para el acceso a la información, considerando quien tiene la necesidad de conocer y los niveles de seguridad, considerando la clasificación de la información.
		5.1.1.8	Considerar la norma legal vigente sobre el acceso a datos o servicios.
		5.1.1.9	Definir formalmente la gestión de derechos de acceso en un ambiente de distribución e interconexión, que reconozca los tipos de conexión disponibles.
		5.1.1.10	Registro de los eventos realizados por el usuario, considerando también a los derechos de acceso privilegiado.
		5.1.1.11	Establecer la regla "Todo está prohibido a no ser que se permita expresamente" en vez de la regla más débil "Todo está permitido a no ser que se prohíba expresamente". Se aplica el principio de menor privilegio

Memorando Nro. MD-DTIC-2021-0114-MEM

Quito, D.M., 08 de junio de 2021

	5.1.2	Acceso a redes y servicios de red Control._ Elaborar, implementar y socializar la política para proveer a los usuarios acceso a las redes y a los servicios de red, para los que han sido específicamente autorizados. Recomendaciones para la implementación:	
		5.1.2.1	Identificar y documentar los equipos que se encuentran en las redes debidamente autorizados.
		5.1.2.2	Procedimientos de autorización que determinen quién tiene permitido el acceso a qué redes y a que servicios de red.
		5.1.2.3	Implementar los controles necesarios para el ingreso a la red y los procedimientos respectivos para proteger el acceso a las conexiones de red y a los servicios de la red.
		5.1.2.4	Políticas para identificar usuarios debidamente autorizados para acceder a las redes y servicios de red a través de VPN, redes virtuales y redes inalámbricas entre otras,
		5.1.2.5	Utilizar métodos para que la identificación del equipo esté en relación a la autenticación del usuario.
		5.1.2.6	Monitorear continuamente el uso de los servicios de la red, con alertas sobre aquellos recursos que se considere críticos.
5.2	Gestión de acceso de los usuarios		
	5.2.1	Registro y retiro de usuarios Control Implementar un procedimiento formal de registro, retiro y modificación de usuarios, con el objetivo de habilitar la asignación de derechos de acceso Recomendaciones para la implementación:	
		5.2.1.1	Establecer un procedimiento formal, documentado y difundido, en el cual se evidencie detalladamente los derechos de acceso,
		5.2.1.2	Definir el administrador de accesos que debe controlar los perfiles y roles,
		5.2.1.3	Gestionar el documento de requerimiento de accesos de los usuarios tanto internos como externos, que contemple; el solicitante del requerimiento o iniciador del proceso, validación del requerimiento, autorizador del requerimiento, ejecutor del requerimiento, forma y medio de entrega del acceso al usuario (manteniendo confidencialidad);
		5.2.1.4	Crear los accesos para los usuarios, para lo cual la institución debe generar convenios de confidencialidad y responsabilidad con el usuario solicitante; además, validar que el usuario tenga los documentos de ingreso con Recursos Humanos (o quien haga estas funciones) en orden y completos.
		5.2.1.5	Modificar los accesos de los usuarios;
		5.2.1.6	Eliminar los accesos de los usuarios;
		5.2.1.7	Suspender temporalmente los accesos de los usuarios en caso de vacaciones, comisiones, licencias, es decir, permisos temporales;
		5.2.1.8	Proporcionar accesos temporales a usuarios externos o terceros de acuerdo al tiempo de su permanencia y limitados según las actividades para las que fueron contratados y firmar un convenio de confidencialidad;
		5.2.1.9	Mantener un registro de la gestión de accesos a aplicaciones, redes, que evidencie, fecha de creación, eliminación, suspensión, activación o eliminación del acceso; al igual que de cada usuario, disponer de los permisos de acceso que han sido asignados.
	5.2.2	Provisión de accesos a usuarios Control Implementar un procedimiento formal para asignar o revocar las credenciales de acceso para todos los tipos de usuarios de todos los sistemas y servicios. Recomendaciones para la implementación:	

Memorando Nro. MD-DTIC-2021-0114-MEM

Quito, D.M., 08 de junio de 2021

		5.2.2.1	Evidenciar documentadamente que cada activo de información tecnológico tenga definido los niveles de acceso basados en perfiles y permisos, a fin de determinar que privilegios se deben asignar según las actividades de los usuarios y la necesidad de la institución y su función;
		5.2.2.2	Verificar que los privilegios asociados con cada servicio o sistema estén de acuerdo con las políticas de acceso y coherente con los requisitos definidos en las funciones que se desempeñan los funcionarios.
		5.2.2.3	Asegurar que las credenciales de acceso no se activen con terceros (proveedores etc.) hasta completar con los procedimientos de autorización;
		5.2.2.4	Mantener un registro documentado de permisos de acceso a sistemas de información y servicios concedidos a un funcionario;
		5.2.2.5	Actualizar las credenciales de acceso de usuarios que han cambiado de rol o de tareas y la eliminación o bloqueo inmediato de los derechos de acceso de los usuarios que han dejado la institución;
		5.2.2.6	Revisar periódicamente las credenciales de acceso a los sistemas de información o de los servicios con los propietarios de los sistemas de información.
	5.2.3	Gestión de Los derechos de acceso con privilegios especiales Control Establecer un proceso formal para funcionarios que tengan la asignación de credenciales de acceso con privilegios especiales; estos deben ser controlados y restringidos. Recomendaciones para la implementación:	
		5.2.3.1	Mantener un cuadro de identificación de los usuarios y sus privilegios especiales asociados con cada servicio o sistema operativo, sistema de gestión de base de datos y aplicaciones;
		5.2.3.2	Las credenciales de acceso con privilegio especial deben asignarse a los usuarios con base en la necesidad de usar y caso a caso de acuerdo con la política de control de acceso, es decir, basados en los requisitos mínimos para el desempeño de sus funciones;
		5.2.3.3	Un proceso de autorización y registro de todos los privilegios especiales asignados. Los niveles de acceso privilegiados no deberían concederse hasta que se complete el proceso de autorización;
		5.2.3.4	Definir las causas para el vencimiento de las credenciales de acceso con privilegio especial.
		5.2.3.5	Las credenciales de acceso con privilegio especial, deben asignarse a un identificador de usuario diferente al usado en las actividades normales de la institución. Las actividades cotidianas de la institución no deberían ser ejecutadas por credenciales con privilegios,
		5.2.3.6	Evaluar continuamente las competencias de los usuarios con credenciales de acceso con privilegios especiales verificando que se correspondan con sus actividades;
		5.2.3.7	Establecer procedimientos específicos para evitar el uso no autorizado de credenciales de usuario administrador genérico en relación con las capacidades de configuración de los sistemas;
		5.2.3.8	Para credenciales de usuario administrador genérico, debería mantenerse la confidencialidad de la información secreta de autenticación cuando esta sea compartida (por ejemplo, cambiando las contraseñas con frecuencia y tan pronto como sea posible cuando un usuario privilegiado deje la institución o cambie de trabajo, comunicándolas a los usuarios privilegiados a través de los mecanismos apropiados).
	5.2.4	Gestión de la información confidencial de autenticación de los usuarios Control Establecer un proceso formal de gestión para la entrega de información confidencial de las credenciales de acceso al sistema y/o servicios. Recomendaciones para la implementación:	

Memorando Nro. MD-DTIC-2021-0114-MEM

Quito, D.M., 08 de junio de 2021

		5.2.4.1	Se debería requerir de los usuarios la firma de un compromiso de mantener la confidencialidad de la información secreta para la autenticación personal y mantener la información de autenticación secreta del grupo (es decir, la compartida) entre los miembros del mismo; este compromiso firmado podría incluirse en los términos y condiciones del acuerdo de confidencialidad del empleo de ser necesario de acuerdo a la gestión institucional,
		5.2.4.2	Cuando la institución requiera que los usuarios mantengan su información de autenticación confidencial, debería proporcionárseles inicialmente una autenticación temporal a ser cambiada obligatoriamente en el primer uso;
		5.2.4.3	Establecer los procedimientos necesarios para verificar la identidad de un usuario antes de proporcionarle la información de autenticación confidencial ya sea nueva, de sustitución o provisional;
		5.2.4.4	La información de autenticación confidencial debería proporcionarse a los usuarios de manera segura; evitando el uso de terceras partes o de correos electrónicos no protegidos (texto sin cifrar);
		5.2.4.5	La información de autenticación secreta temporal debería ser única para el individuo y no debería poder predecirse;
		5.2.4.6	Utilizar el procedimiento adecuado para que los usuarios confirmen la recepción de la información de autenticación confidencial;
		5.2.4.7	La información de autenticación confidencial entregada por el proveedor, debería cambiarse tras la instalación de los sistemas o del software.
	5.2.5	Revisión de los derechos de acceso de usuario Control Los propietarios de los activos deberán revisar o coordinar la revisión de los derechos de acceso, a intervalos regulares definidos por la institución. Recomendaciones para la implementación;	
		5.2.5.1	Las credenciales de acceso del usuario deben revisarse al menos cada 90 días o de acuerdo a las necesidades de la institución y tras cualquier cambio institucional o de funciones de los usuarios.
		5.2.5.2	La asignación de privilegios debe verificarse al menos cada 30 días o de acuerdo a las necesidades de la institución, para asegurar que no se han obtenido privilegios no autorizados;
		5.2.5.3	Los cambios en cuentas de usuarios deben registrarse en los logs de los sistemas de gestión de información para su revisión periódica.
	5.2.6	Retiro o adaptación de los derechos de acceso Control Retirar los privilegios de acceso a los empleados y usuarios de terceras partes a la información y a las instalaciones de procesamiento de información (ej., sistema de directorio, correo electrónico, accesos físicos, aplicaciones de software, etc.,) inmediatamente luego de que se comunique la terminación de la relación laboral por parte del área correspondiente. Recomendaciones para la implementación: Retirar los derechos de acceso a la información y los activos asociados a las instalaciones de procesamiento de la información deberían restringirse o eliminarse antes de que el empleado finalice o cambie de puesto de trabajo, dependiendo de la evaluación de factores de riesgo como:	
		5.2.6.1	Si el funcionario presenta su renuncia o solicita su cambio de área, así como la razón para la finalización.
		5.2.6.2	Las responsabilidades del funcionario, y de cualquier usuario el momento de la renuncia o cambio.

Memorando Nro. MD-DTIC-2021-0114-MEM

Quito, D.M., 08 de junio de 2021

		5.2.6.3	El valor de los activos a los que han tenido acceso el momento de renuncia o cambio.	
5.3	Responsabilidades del usuario			
	5.3.1	Uso de la información confidencial para la autenticación Control Elaborar la política, implementarla y socializar a los usuarios las responsabilidades del uso de las credenciales de acceso a la información y a los equipos puestos a su disposición. Recomendaciones para la implementación:		
		5.3.1.1	Mantener la confidencialidad de la información de autenticación, asegurando su no divulgación, incluyendo a personas con autoridad;	
		5.3.1.2	Evitar guardar (por ejemplo, en papel, en un fichero software o en un dispositivo portátil) las credenciales de acceso, a no ser que esta pueda ser almacenada de forma segura y que el método de almacenamiento haya sido aprobado (por ejemplo, en repositorios seguros para contraseñas);	
		5.3.1.3	Cambiar las contraseñas de autenticación siempre que haya indicios de su posible divulgación;	
		5.3.1.4	Cuando se usen contraseñas como información secreta de autenticación, seleccionar contraseñas de calidad con una longitud mínima de 8 caracteres que:	
			5.3.1.4.1	Sean fáciles de recordar,
			5.3.1.4.2	Que no estén basadas en algo que alguien más pueda adivinar con facilidad u obtener usando información asociada a la persona, por ejemplo, nombres, números de teléfono, fechas de nacimiento, etc.,
			5.3.1.4.3	Que no sea vulnerable a ataques de diccionario (es decir, que no consista en palabras incluidas en diccionarios),
			5.3.1.4.4	Que estén libres de caracteres consecutivos bien sean todos numéricos o todos alfabéticos,
			5.3.1.4.5	Si es temporal, que sea cambiada en el primer inicio de sesión,
		5.3.1.5	Asegurar una protección adecuada de las contraseñas cuando estas sean usadas como información secreta de autenticación y almacenadas en procesos automáticos de inicio de sesión;	
		5.3.1.6	No usar las mismas contraseñas de autenticación para propósitos laborales y privados.	
		5.3.1.7	El Oficial de Seguridad de la información deberá gestionar actividades periódicas (una vez cada mes como mínimo) para la revisión al contenido de las pantallas de los equipos, con el fin de que no se encuentren iconos y accesos innecesarios, y carpetas y archivos que deben ubicarse en la carpeta de documentos del usuario.	
5.4	Control de acceso a sistemas y aplicaciones			
	5.4.1	Restricción del acceso a la Información Control Restringir el acceso de los usuarios a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida. Recomendaciones para la implementación:		
		5.4.1.1	Control del acceso a las funciones del sistema de aplicaciones;	
		5.4.1.2	Monitorear cuales son los datos a los que acceda un usuario determinado, de acuerdo al perfil definido;	
		5.4.1.3	Implementar controles sobre los perfiles de acceso de los usuarios, por ejemplo, de lectura, de escritura, de borrado y de ejecución de la información, etc.;	
		5.4.1.4	Implementar controles para el ingreso a otras aplicaciones de acuerdo a los perfiles de usuario determinados.	
		5.4.1.5	Generar revisiones periódicas de las salidas de los sistemas de aplicación para garantizar el retiro de la información redundante.;	

Memorando Nro. MD-DTIC-2021-0114-MEM

Quito, D.M., 08 de junio de 2021

		5.4.1.6	Implementar controles de acceso tanto físico o lógico para aislar las aplicaciones sensibles, los datos de aplicación o los sistemas. (DMZ).
	5.4.2	Procedimientos seguros de inicio de sesión Control Implementar un procedimiento seguro de inicio de sesión cuando se requiera una autenticación robusta, para controlar el acceso a los sistemas y aplicaciones institucionales por ejemplo medios criptográficos, tarjetas inteligentes, dispositivos hardware o medios biométricos Recomendaciones para la implementación:	
		5.4.2.1	Controlar que no se muestren identificadores del sistema o aplicación hasta que el proceso de inicio de sesión se haya completado con éxito;
		5.4.2.2	Socializar un aviso general de que únicamente deben acceder al computador los usuarios autorizados;
		5.4.2.3	Evitar que se desplieguen mensajes de ayuda durante el proceso de inicio de sesión que pudieran ayudar a un usuario no autorizado;
		5.4.2.4	Validar la información de inicio de sesión solo cuando se hayan registrado todos los datos de entrada. Sí ocurre alguna condición de error, el sistema no debería indicar qué parte del dato es correcto o incorrecto;
		5.4.2.5	Limitar la cantidad de intentos permitidos de registro de inicio de sesión; por ejemplo, tres intentos;
		5.4.2.6	Llevar un proceso de monitoreo y registro de los intentos exitosos y fallidos de autenticación del sistema, registros de alarmas cuando se violan las políticas de seguridad del sistema, generando la alerta respectiva;
		5.4.2.7	Mostrar la siguiente información tras completar con éxito el inicio de sesión:
		5.4.2.8	No exponer la contraseña que se está introduciendo;
		5.4.2.9	No transmitir por la red contraseñas sin cifrar;
		5.4.2.10	Terminar las sesiones inactivas tras un período definido de tiempo de inactividad, especialmente en lugares de alto riesgo, como áreas públicas o externas que queden fuera de la gestión de la seguridad de la institución o en dispositivos móviles;
		5.4.2.11	Restringir los tiempos de conexión para proporcionar una seguridad adicional a las aplicaciones de alto riesgo y reducir la ventana de oportunidad para accesos no autorizados.
	5.4.3	Sistema de gestión de contraseñas Control Elaborar la política para la gestión de contraseñas, debe ser interactiva y asegurar la calidad de las mismas. Recomendaciones para la implementación:	
		5.4.3.1	Evidenciar en la política de accesos, la responsabilidad del buen uso de la contraseña y que debe ser secreta e intransferible para mantener la responsabilidad;
		5.4.3.2	Permitir a los usuarios escoger y cambiar sus propias contraseñas e incluir un procedimiento de confirmación que tenga en cuenta los errores de entrada;
		5.4.3.3	Imponer la complejidad de contraseñas para asegurar el ingreso a los sistemas;
		5.4.3 4	Forzar a los usuarios el cambio de contraseña en el primer inicio de sesión;
		5.4.3.5	Forzar a los usuarios el cambio regular de contraseñas, del personal de tecnología, de los administradores de tecnología, en rangos de tiempo y complejidad y cuando sea necesario;
		5.4.3.6	Mantener un registro de las contraseñas usadas anteriormente y evitar su re utilización, especialmente en activos críticos;

Memorando Nro. MD-DTIC-2021-0114-MEM

Quito, D.M., 08 de junio de 2021

		5.4.3.7		No mostrar las contraseñas en la pantalla cuando el usuario este ingresando; 5.4.3.8 Generar un procedimiento formal para la administración y custodia de las contraseñas de acceso de administración e información de la institución, de manera separada de los datos del sistema.
		5.4.3.9		Almacenar y transmitir las contraseñas en formatos protegidos (encriptados o codificados).
		5.4.3.10		Documentar el control de acceso para los usuarios temporales.
		5.4.3.11		Generar y documentar revisiones periódicas de la gestión de usuarios incluidos los administradores de tecnología, por parte del Oficial de Seguridad de la Información.
	5.4.4	Uso de herramientas de administración de sistemas Control El uso de programas utilitarios o software que puedan ser capaces de anular o evitar los controles del sistema y aplicaciones, deben ser restringidos y fuertemente controlados. Recomendaciones para la implementación:		
		5.4.4.1		Uso de procedimientos de identificación, autenticación y autorización para los programas utilitarios;
		5.4.4.2		Separación de los programas utilitarios del software de aplicaciones;
		5.4.4.3		Limitación del uso de programas utilitarios a la cantidad mínima viable de usuarios de confianza autorizados;
		5.4.4.4		Autorización del uso de programas utilitarios, no estandarizados en la institución
		5.4.4.5		Limitar la disponibilidad de los programas utilitarios, por ejemplo, a la duración de un cambio autorizado;
		5.4.4.6		Registrar todo uso de programas utilitarios;
		5.4.4.7		Definir y documentar los niveles de autorización para los programas utilitarios de administración;
		5.4.4.8		Retirar, eliminar o inhabilitar todos los programas utilitarios que sean innecesarios;
	5.4.5	Control de acceso al código fuente del programa Control Restringir el acceso al código fuente de las aplicaciones software, programas, de acuerdo a las políticas establecidas por la institución. Recomendaciones para la implementación,		
		5.4.5.1		Asignar a un administrador del código fuente de programas, software, quien tendrá en custodia los mismos y deberá:
			5.4.5.1.1	Utilizar un manejador de versiones para el código fuente, proporcionar permisos de acceso a los desarrolladores bajo autorizaciones.
			5.4.5.1.2	Proveer al área de Desarrollo los programas fuentes solicitados para su modificación, manteniendo en todo momento la correlación programa fuente/ejecutable.
			5.4.5.1.3	Llevar un registro actualizado de todos los programas fuentes en uso, indicando nombre del programa, programador, autorizador versión, fecha de última modificación y fecha/hora de compilación y estado (en modificación o en producción).
			5.4.5.1.4	Verificar que el autorizador de la solicitud de un programa fuente sea el designado para la aplicación, rechazando el pedido en caso contrario.
			5.4.5.1.5	Registrar cada solicitud aprobada.
			5.4.5.1.6	Administrar las distintas versiones de una aplicación.

Memorando Nro. MD-DTIC-2021-0114-MEM

Quito, D.M., 08 de junio de 2021

			5.4.5.1.7	Asegurar que un mismo programa fuente no sea modificado simultáneamente por más de un desarrollador, sin un manejador de versiones.
			5.4.5.1.8	Realizar las copias de respaldo de los programas fuentes cumpliendo los requisitos de seguridad establecidos como respaldos de información.
		5.4.5.2	Cuando sea posible, las librerías de programas fuente no deben guardarse en los sistemas en producción o en explotación;	
		5.4.5.3	El código fuente de programas y las librerías fuente de programas se deberán gestionar de acuerdo con los procedimientos establecidos;	
		5.4.5.4	El personal de soporte no debe tener acceso sin restricciones al código de programas fuente.	
		5.4.5.5	La actualización del código fuente de programas y de los elementos asociados, así como la emisión de fuentes de programa a los programadores, solamente se deberá efectuar después de recibir la autorización respectiva;	
		5.4.5.6	Los listados del código de programa deben guardarse en un entorno seguro;	
		5.4.5.7	Conservar un registro para auditoría de todos los accesos al código fuente de programas;	
		5.4.5.8	El mantenimiento y el copiado del código fuente de programas deberán estar sujetos a un procedimiento estricto de control de cambios.	

• Las NORMAS DE CONTROL INTERNO DE LA CONTRALORÍA GENERAL DEL ESTADO, disponen:
"410-12 Administración de soporte de tecnología de información
La Unidad de Tecnología de Información definirá, aprobará y difundirá procedimientos de operación que faciliten una adecuada administración del soporte tecnológico y garanticen la seguridad, integridad, confiabilidad y disponibilidad de los recursos y datos, tanto como la oportunidad de los servicios tecnológicos que se ofrecen.
410-04 Políticas y procedimientos
La máxima autoridad de la entidad aprobará las políticas y procedimientos que permitan organizar apropiadamente el área de tecnología de información y asignar el talento humano calificado e infraestructura tecnológica necesaria.
La Unidad de Tecnología de Información definirá, documentará y difundirá las políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de información y comunicaciones en la organización, estos se actualizarán permanentemente e incluirán las tareas, los responsables de su ejecución, los procesos de excepción, el enfoque de cumplimiento y el control de los procesos que están normando, así como, las sanciones administrativas a que hubiere lugar si no se cumplieran."

• La Secretaría del Deporte mediante Resolución Nro. 0007, resuelve expedir la REFORMA L ESTATUTO ORGÁNICO DE GESTIÓN ORGANIZACIONAL POR PROCESOS DE LA SECRETARIA DEL DEPORTE publicado mediante Resolución No. 0034, expedida el 20 de junio de 2016, publicado en el Registro Oficial No. 808 de 29 de julio de 2016, y resolución Nro. 0030 de 20 de mayo de 2020, donde señala:
*"**Gestión interna de infraestructura de TIC:***
(…)
1.Manual de procedimientos para asignación, actualización y revocación de cuentas y perfiles de usuarios en las aplicaciones, sistemas y servicios tecnológicos y sus modificaciones.
3.Diagramas de aplicaciones y arquitecturas de servidores, redes LAN/WAN/WIRELESS, interconexión, almacenamiento, respaldo y recuperación, centralización y virtualización.
6.Informes de seguimiento y control, así como también de las medidas de prevención y recuperación de servicios de TIC.
11.Reportes de controles de acceso a los sistemas y servicios informáticos (…)"

Memorando Nro. MD-DTIC-2021-0114-MEM

Quito, D.M., 08 de junio de 2021

*"**Gestión interna de seguridad informática de TIC:***
(…)
2.Políticas de seguridad informática y de la información y su actualización.
3.Matriz de clasificación en diferentes niveles de seguridad según sean: contratistas-contratantes, administradores y usuarios de los diferentes sistemas, servicios y soluciones tecnológicas.
4.Informe de seguimiento y control de prevención de ataques informáticos a aplicaciones, servicios y sistemas informáticos
8.Catálogo de procedimientos para asignación, actualización y revocación de cuentas y perfiles de usuarios en las aplicaciones, sistemas y servicios informáticos.
(…)"

- Mediante memorando Nro. MD-DTIC-2017-0210 de 11 de septiembre de 2017, la Dirección de Tecnologías de la Información y Comunicación designa a la Ing. Vilma Ávila como responsable de la Gestión de Infraestructura Tecnológica.

- Mediante memorando Nro. MD-DTIC-2017-0211 de 11 de septiembre de 2017, la Dirección de Tecnologías de la Información y Comunicación designa a la Ing. Andrea Valdivieso como responsable de la Gestión Interna de Seguridad, Interoperabilidad y Riesgos.

En virtud de lo expuesto y con el fin de dar cumplimiento a lo dispuesto por los Organismo de Control, solicito se remita la documentación actualizada que da cumplimiento a los parámetros antes descritos, información que deberá ser entregada hasta el 30 de junio de 2021; en el caso de no disponer de toda la documentación se deberá presentar un cronograma de trabajo que permita cumplir con el 100% de requerimientos.

Particular que comunico para los fines pertinentes.

Atentamente,

Documento firmado electrónicamente

Ing. Juan Pablo Cevallos Peñafiel
DIRECTOR DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Anexos:
- md-dtic-2017-0210072150100162275600 3.pdf
- md-dtic-2017-0211006817400162275600 4.pdf
- snap-snadp-2013-000227-o0149560001622755987.pdf

Copia:
Sr. Mgs. Daniel David Uribe Pupiales
Asistente de Tecnologías de la Información

du

Firmado electrónicamente por:
JUAN PABLO CEVALLOS PENAFIEL