MINISTERIO DE DEFENSA NACIONAL

POLÍTICA

de Control de Acceso a los Sistemas de Informarción

SUBSECRETARIA DE DEFENSA

República del Ecuador

Gobierno del Encuentro | Juntos lo logramos

Información del Documento

HISTORIA DEL DOCUMENTO			
Nombre del Documento	POLÍTICA DE CONTROL DE ACCESO A LOS SISTEMAS DE INFORMACIÓN		
Elaborado por:	MAYOR-VALLEJO PATRICIO		
Unidad responsable	Subsecretaria de Defensa	**Fecha de Elaboración:**	18-JUN-020

CONTROL DE VERSIONES			
Versión	**Fecha de creación**	**Preparado por:**	**Descripción**
1.1	18-JUN-020	Mayor. Vallejo	Con base a las Políticas de Seguridad del EGSI del Ministerio de Defensa Nacional

DIRECCIÓN: Calle la Exposición S4-71 y Benigno Vela **Código Postal:** 170403 / Quito – Ecuador **Teléfono:** 593-2 298-3200

www.defensa.gob.ec

TABLA DE CONTENIDOS

DIRECCIÓN: Calle la Exposición S4-71 y Benigno Vela **Código Postal:** 170403 / Quito – Ecuador **Teléfono:** 593-2 298-3200

www.defensa.gob.ec

SECCIÓN I VISIÓN GENERAL

El presente documento tiene como objeto reconocer la importancia y el valor de la información con respecto al funcionamiento eficiente y efectivo del Ministerio de Defensa Nacional, considerando como premisa que la información no es sólo crítica para el éxito de esta Cartera de Estado, sino estratégica, que permite garantizar la confidencialidad, integridad y disponibilidad de la información.

1. Antecedentes

Registro Oficial N° 228 del Ministerio de Telecomunicaciones y de la sociedad de la Información, de fecha 10 de enero de 2020, en la cual se expide el Esquema Gubernamental de Seguridad de la Información EGSI v2.0.

Acuerdo Ministerial Nº 134 del Ministerio de Defensa Nacional, mediante el cual se expide la Directiva para la Implementación del Esquema Gubernamental de Seguridad de la Información para todas las Instituciones Dependientes y Adscritas al sector Defensa.

Las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27001: 2013, TECNOLOGÍAS DE LA INFORMACIÓN — TÉCNICAS DE SEGURIDAD — SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

Políticas de Seguridad de la Información del Ministerio de Defensa Nacional.

2. Objetivos

Objetivo General:

Planear, organizar, dirigir y controlar el acceso y uso aceptable de todo el equipamiento computacional, servicios y sistemas de información, así como de las redes de datos del Ministerio de Defensa.

3. Alcance

Las políticas contenidas en este documento, son de aplicación obligatoria para los Servidores y Trabajadores civiles y militares que laboren o presten servicios en esta Cartera de Estado; así como, para cualquier persona externa que de una u otra forma utilice las tecnologías de información y comunicaciones del Ministerio de Defensa Nacional.

DIRECCIÓN: Calle la Exposición S4-71 y Benigno Vela **Código Postal:** 170403 / Quito – Ecuador **Teléfono:** 593-2 298-3200

www.defensa.gob.ec

4. Definiciones

Derechos privilegiados: Conjunto de permisos o atributos dados a un usuario, quien de acuerdo con sus funciones y/o tareas encomendadas, puede acceder a un determinado recurso.

Restricciones de acceso: Delimitar el acceso de los usuarios a determinados recursos.

5. Roles y responsabilidades

Oficial de Seguridad de la Información

Ejecutar labores de coordinación para una adecuada elaboración, revisión e implementación de esta política y las materias que ella comprende.

Comité de Seguridad de la Información

Asegurar que las materias abordadas en esta política se ejecutan y se cumplen, identificar como se manejan los no cumplimientos, promover la difusión y sensibilización de las materias abordadas en este documento, revisar periódicamente la política detectando y proponiendo mejoras.

Dirección de Tecnologías de la Información

Evaluar e implementar en caso de ser factible las propuestas de Seguridad, así como revisar periódicamente la política detectando y proponiendo mejoras. Tiene a cargo el otorgamiento de acceso a los recursos de red.

Encargado de receptar, evaluar y configurar las solicitudes de registro de usuarios, permisos de acceso, perfiles y accesos privilegiados a los servicios y sistemas de información, de acuerdo a las normas, políticas, directicas e instructivos vigentes en coordinación con el Asesor Militar de Seguridad de la Información de esta Cartera de Estrado (OSI)

Servidores y Trabajadores civiles y militares

Cumplir cabalmente con las disposiciones y requerimientos establecidos en la presente política. Cada usuario de la información, equipos informáticos y de los servicios de red de esta Cartera de Estado deberá velar por la correcta implementación de las normas de control de acceso promovidas por la Institución, dentro de sus áreas de responsabilidad, así como del cumplimiento por parte de su equipo de trabajo.

DIRECCIÓN: Calle la Exposición S4-71 y Benigno Vela **Código Postal:** 170403 / Quito – Ecuador **Teléfono:** 593-2 298-3200

www.defensa.gob.ec

SECCIÓN II POLÍTICAS

1. Política de control de acceso

1.1. Perspectiva

Con el objetivo de proteger la información de la institución previniendo el acceso no autorizado a los equipos y sistemas informáticos del Ministerio de Defensa, los usuarios de los sistemas de información de la institución deben poseer una cuenta personal que lo identifique. La identificación se realizará normalmente por un nombre de usuario único (Username) y una contraseña (Password).

2. Política de control de acceso a los sistemas de información

De aplicación a todos los funcionarios civiles y militares, usuarios externos y terceras partes que por la naturaleza de sus funciones requieren acceso a la información de Esta Cartera de Estado. Describe las consideraciones generales sobre la protección y el control de acceso a la información para evitar el acceso no autorizado a sistemas y/o servicios, y hacer que los usuarios rindan cuentas por la administración y protección de su información y sus claves.

2.1. Obligaciones

Todo el personal militar, servidores y trabajadores públicos del Ministerio de Defensa, incluso terceros, deben tener acceso sólo a la información que necesitan de acuerdo al rol y perfil que cumple dentro de la organización de la Institución.

Para el desarrollo legítimo de sus funciones y actividades dentro de la institución, la asignación de privilegios y acceso a los activos de información (correo electrónico institucional, software, aplicaciones, carpetas compartidas, etc.) deben estar basados en las necesidades de las áreas y aprobados por el propietario de los activos, los mismos que son validados y aprobados por la Dirección de Tecnologías de la Información.

Para todo medio de procesamiento de información al que se necesite conceder accesos como: servidores, aplicaciones, carpetas compartidas, base de datos, etc., se lo realizará previa solicitud a la Dirección de Tecnologías de la Información a través de la Coordinación Administrativa Financiera, quienes previo análisis autorizarán los permisos de acceso previo a la legalización de un documento de respaldo.

DIRECCIÓN: Calle la Exposición S4-71 y Benigno Vela **Código Postal:** 170403 / Quito – Ecuador **Teléfono:** 593-2 298-3200

www.defensa.gob.ec

Sólo se pueden conceder accesos a personal externo a la institución, previa solicitud por escrito del director o Autoridad Jerárquica responsable del activo de información. Las cuentas de acceso a terceros deben tener especificado un tiempo de expiración, el que debe ser controlado por la Dirección de Tecnologías de la Información.

Cualquier intento de acceso no autorizado a los equipos, carpetas compartidas, sistemas de información será considerado un incidente grave, por lo que debe reportar al Oficial de Seguridad de la Información a través de la Subsecretaria de Defensa, quien a su vez de forma coordinada con la Dirección de Tecnologías de la Información, analizará el incidente conforme a lo establecido en las Políticas de Seguridad de la Información.

3. Acceso a las redes y a los servicios de la red

Asegurar que sólo usuarios autorizados tengan acceso a los servicios e infraestructura de esta Cartera de Estado a fin de prevenir cualquier daño físico o interferencia con los activos de información.

3.1. Obligaciones

El acceso a los sistemas y servicios de red de la Institución es otorgado sólo a usuarios identificados y autentificados para todos los sistemas de información del Ministerio de Defensa. Para el efecto el usuario deberá identificarse a fin de comprobar su autentificación.

Los usuarios deben tener acceso a la red y a los servicios de la red para los que han sido autorizados específicamente, lo cual debe quedar establecido en la asignación de privilegios correspondiente.

La cuenta de usuario y la contraseña son individuales e instranferibles.

La autenticación en sistemas por parte de los usuarios y administradores deben ser registrados en los logs para actividades de auditoria y eventuales análisis forenses.

4. Uso de información calificada

Asegurar que sólo usuarios autorizados tengan acceso a información calificada según corresponda, así como establecer y normar el tratamiento que se brindará a la misma.

DIRECCIÓN: Calle la Exposición S4-71 y Benigno Vela **Código Postal:** 170403 / Quito – Ecuador **Teléfono:** 593-2 298-3200

www.defensa.gob.ec

4.1. Obligaciones

Está prohibido el uso de un nombre de usuario ajeno o facilitar la cuenta de usuario y su contraseña personal a un tercero.

Queda absolutamente prohibido anotar las contraseñas de acceso en lugares visibles o públicos.

Las credenciales (usuario y contraseña) no deben ser incluidos en aplicaciones donde puedan quedar expuestas (macros de planillas, documentos o programas de tipo script).

La composición de las contraseñas debe tener un mínimo de 8 caracteres, alfanumérica, fáciles de recordar, que no se basen en nada que otra persona pueda adivinar u obtener fácilmente mediante la información relacionada con el dueño de la cuenta, que no sean vulnerables a ataques de diccionario (es decir, que no conste de palabras incluidas en los diccionarios).

El usuario deberá cambiar la información de autenticación secreta cuando exista algún indicio de una posible vulneración.

El usuario no utilizará las mismas contraseñas para fines laborales y personales.

5. Registro de eventos

Establecer y normar las consideraciones para realizar un adecuado monitoreo en las instalaciones de procesamiento de la información y usuarios que acceden a los activos de información de esta Cartera de Estado, debiendo generar, mantener y revisar registros de las actividades de los usuarios: excepciones, faltas y eventos de seguridad de la información de manera regular.

5.1. Obligaciones

La Dirección de Tecnologías de la Información es la encargada de los activos informáticos bajo su responsabilidad, por lo que son los responsables de colaborar en el control y efectuar recomendaciones de mejora permanente.

Los registros de eventos deben considerar, entre otros los siguiente:

- ID de usuarios.
- Actividades del sistema.
- Fecha, horas y detalles de los eventos clave, es decir, el inicio y finalización de la sesión.

DIRECCIÓN: Calle la Exposición S4-71 y Benigno Vela **Código Postal:** 170403 / Quito – Ecuador **Teléfono:** 593-2 298-3200

www.defensa.gob.ec

- Los registros de los intentos exitosos y rechazados de acceso al sistema.
- Las direcciones y protocolos de redes.

6. Registros de actividad del administrador y operador del sistema

Establecer y normar las consideraciones para realizar un adecuado monitoreo y respaldo del administrador y operadores de los sistemas tecnológicos de esta Cartera de Estado.

6.1. Obligaciones

La Dirección de Tecnologías de la Información deberá registrar, respaldar, proteger y revisar regularmente, las actividades del administrador y operadores de las distintas plataformas tecnológicas. El Log de actividades debe incluir al menos:

- Identificación del equipo.
- Horario de arranque y finalización de los procesos del sistema.
- Errores del sistema y acciones críticas realizadas.
- Cuenta del usuario que realizó la actividad

7. Registros de usuarios y retiros de cuentas

Establecer y normar las consideraciones para realizar un adecuado procedimiento que permita la creación y eliminación de cuentas de los usuarios que tendrán acceso a los diferentes sistemas tecnológicos de esta Cartera de Estado.

7.1. Obligaciones

El personal de administradores de los sistemas y aplicaciones pertenecientes a la Dirección de Tecnologías de la Información, previa solicitud por escrita de la Dirección de Talento Humano realizarán la creación de la(s) cuenta(s) de usuario(s) con la ayuda de las herramientas según el rol y función que cumplirán.

El personal de administradores de los sistemas y aplicaciones pertenecientes a la Dirección de Tecnologías de la Información, previamente comunicado por la Dirección de Talento Humano, procederán a desactivar o eliminar la cuenta solicitada del personal militar, servidores y trabajadores públicos del Ministerio de Defensa, dejando como constancia la firma de la Hoja de Salida de la Institución.

DIRECCIÓN: Calle la Exposición S4-71 y Benigno Vela **Código Postal:** 170403 / Quito – Ecuador **Teléfono:** 593-2 298-3200

www.defensa.gob.ec

El personal de administradores de los sistemas y aplicaciones pertenecientes a la Dirección de Tecnologías de la Información, bloquearán temporalmente las cuentas de usuarios del personal militar, servidores y trabajadores públicos en caso de determinar una violación o intromisión a la seguridad de los activos de información de Esta Cartera de Estado.

8. Gestión de los derechos de acceso con privilegios especiales

Establecer y normar las consideraciones para entregar permisos especiales sobre el manejo de las herramientas tecnológicas sobre las que maneja la información de esta Cartera de Estado.

8.1. Obligaciones

La solicitud de una cuenta de usuario privilegiado debe ser solicitada de manera escrita a la Coordinación Administrativa Financiera para su análisis y aprobación por parte de la Dirección de Tecnologías de la Información en coordinación con el Oficial de Seguridad de la Información de esta esta Cartera de Estado. La misma que deberá ir acompañada de una justificación de necesidad de uso. Debiendo legalizar un acta de responsabilidad y confidencialidad.

Las cuentas de usuario privilegiado sólo deben ser otorgadas a personal que ha sido autorizado por necesidad laboral por parte de los señores Subsecretarios y Coordinadores de acuerdo al cumplimiento de las funciones asignadas al usuario.

La Dirección de Tecnologías de la Información debe disponer de un procedimiento para la asignación, uso y revocación de cuentas de usuario privilegiado.

Los accesos realizados con cuentas de usuario privilegiados serán registrados y controlados periódicamente por parte de la Dirección de Tecnologías de la Información.

Una cuenta de usuario privilegiado sólo podrá ser utilizada por el usuario solicitante y que requiere dichos privilegios y con fines laborables, no podrá ser utilizada en actividades rutinarias o personales.

DIRECCIÓN: Calle la Exposición S4-71 y Benigno Vela **Código Postal:** 170403 / Quito – Ecuador **Teléfono:** 593-2 298-3200

www.defensa.gob.ec

PERIODICIDAD DE EVALUACIÓN Y REVISIÓN

La presente política debe ser evaluada cada año o cada vez que se modifiquen las Políticas de Seguridad de la Información del Ministerio de Defensa Nacional.

FIRMAS DE RESPONSABILIDAD

Elaborado Por:	MAYO. Patricio Vallejo, OSI	Firmado electrónicamente por: ROBERTO PATRICIO VALLEJO ALMEIDA
Revisado Por	Ing. Grace Miranda, Directora de TICs.	Firmado electrónicamente por: GRACE LILIAN MIRANDA ESCOBAR
Autenticado Por:	CRNL. Rodrigo Ordoñez, Presidente del CSI	Firmado electrónicamente por: RODRIGO FERNANDO ORDOÑEZ LOZADA
Aprobado Por:	CALM. Pablo Caicedo Sub Secretario de Defensa.	Firmado electrónicamente por: PABLO IVAN CAICEDO SALVADOR

DIRECCIÓN: Calle la Exposición S4-71 y Benigno Vela **Código Postal:** 170403 / Quito – Ecuador **Teléfono:** 593-2 298-3200

www.defensa.gob.ec