Controles NCH ISO 27001:2013 Relacionados

CONTROL	NOMBRE
A.14.01.02	Aseguramiento de servicios de aplicación en redes
A.14.01.03	Protección de transacciones de servicios de aplicación
A.14.02.01	Política de desarrollo seguro
A.14.02.02	Procedimientos de control de cambios
A.14.02.03	Revisión técnica de las aplicaciones después de los cambios en la plataforma de operaciones
A.14.02.04	Restricción en los cambios a los paquetes de software
A.14.02.05	Principios de ingeniería de sistema seguro
A.14.02.06	Entorno de desarrollo seguro
A.14.02.07	Desarrollo tercerizado
A.14.02.08	Prueba de seguridad del sistema
A.14.02.09	Prueba de aprobación del sistema
A.14.03.01	Protección de datos de prueba

Control de Versiones

FECHA	VERSIÓN	RESPONSABLES	DESCRIPCIÓN
28-06-2019	1.0	Jorge Romero Vargas Solange Godoy Carrera	Elaboración de documento
02-11-2020	1.1	Jorge Romero	Mejoras en la redacción. Incluye uso de repositorio de software para el control de versiones, en sección de desarrollo de software seguro. Se menciona el uso de características de tipo impersonate en ambiente exclusivamente de pruebas.
30-11-2021	1.2	Jorge Romero	Actualización sección firmantes. Menciona mecanismo de control de firmas digitalizadas en documentos. Incorpora control 14.1.3 Protección de las transacciones de servicio de aplicación.
04-11-2022	1.3	Jorge Romero	Actualización sección firmantes. Incluye normativa para definición de portales en sus distintos ambientes. Incorpora buenas prácticas en el uso de repositorios y autenticación desde aplicaciones y portales. Establece matriz de registro y control de los requerimientos.
11-08-2023	1.4	Jorge Romero	Modifica Jefe Unidad de Tecnologías de la Información por Encargado Área de Tecnologías de la Información. Modifica Unidad de Tecnologías de la Información por Área de Tecnologías de la Información.

1. Introducción

El Ministerio Secretaría General de la Presidencia, en adelante el "Ministerio", dispone del presente documento, "Política de Desarrollo", como parte integrante del sistema de seguridad de la información.

En específico, la presente política se enmarca en el cumplimiento de la NCH ISO 27001, que propone como requisito de control:

Control A.14.01.02 Aseguramiento de servicios de aplicación en redes públicas

"La información relacionada a servicios de aplicación que pasan por redes públicas debe ser protegida de la actividad fraudulenta, disputas contractuales, y su divulgación y modificación no autorizada".

- Requisito de control A.14.01.02 NCH ISO 27001-2013.

Control A.14.01.03 Protección de transacciones de servicios de aplicación

"La información implicada en transacciones servicio de aplicación se debe proteger para evitar la transmisión incompleta, la omisión de envío, la alteración no autorizada del mensaje, la divulgación no autorizada, la duplicación o repetición no autorizada del mensaje".

- Requisito de control A.14.01.03 NCH ISO 27001-2013.

Control A.14.02.01 Política de desarrollo seguro

"Las reglas para el desarrollo de software y de sistemas deben ser establecidas y aplicadas a los desarrollos dentro de la organización".

- Requisito de control A.14.02.01 NCH ISO 27001-2013.

Control A.14.02.02 Procedimientos de control de cambios del sistema

"Los cambios a los sistemas dentro del ciclo de desarrollo deben ser controlados mediante el uso de procedimientos formales de control de cambios".

- Requisitos de control A.14.02.02 NCH ISO 27001-2013.

Control A.14.02.03 Revisión técnica de las aplicaciones después de los cambios en la plataforma de operación

"Cuando se cambien las plataformas de operación, se deben revisar y poner a prueba las aplicaciones críticas del negocio para asegurar que no haya impacto adverso en las operaciones o en la seguridad de la organización".

- Requisito de control A.14.02.03 NCH ISO 27001-2013.

Control A.14.02.04 Restricciones en los cambios a los paquetes de software

"Se debe desalentar la realización de modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, los que deben ser controlados de manera estricta".

- Requisito de control A.14.02.04 NCH ISO 27001-2013.

Control A.14.02.05 Principios de ingeniería de sistema seguro
"Se deben establecer, documentar, mantener y aplicar principios para los sistemas seguros de ingeniería para todos los esfuerzos de implementación de sistema de información".
- Requisito de control A.14.02.05 NCH ISO 27001-2013.

Control A.14.02.06 Entorno de desarrollo seguro
"Las organizaciones deben establecer y proteger los entornos de desarrollo seguro, de manera apropiada, para el desarrollo del sistema y los esfuerzos de integración que cubren todo el ciclo de desarrollo del sistema".
- Requisito de control A.14.02.06 NCH ISO 27001-2013.

Control A.14.02.07 Desarrollo tercerizado
"La organización debe supervisar y monitorear la actividad del desarrollo del sistema tercerizado".
- Requisito de control A.14.02.07 NCH ISO 27001-2013.

Control A.14.02.08 Prueba de seguridad del sistema
"Durante el desarrollo se debe realizar la prueba de funcionalidad de seguridad".
- Requisito de control A.14.02.08 NCH ISO 27001-2013.

Control A.14.02.09 Prueba de aprobación del sistema
"Se deben definir los programas de prueba de aceptación y los criterios pertinentes para los nuevos sistemas de información, actualizaciones y versiones nuevas".
- Requisito de control A.14.02.09 NCH ISO 27001-2013.

Control A.14.03.01 Protección de datos de prueba
"Los datos de prueba se deben seleccionar, proteger y controlar de manera muy rigurosa".
- Requisito de control A.14.03.01 NCH ISO 27001-2013.

2. Alcance

Esta política debe aplicarse en el proceso de desarrollo de software del Ministerio, estableciendo reglas para los desarrolladores, alumnos/as en prácticas, desarrolladores externos y equipos tecnológicos con el fin de resguardar el manejo de la información, aplicando buenas prácticas para una construcción segura de software.

3. Objetivo

El Ministerio deberá llevar a cabo principios de desarrollo de software seguro, aplicando los controles que sean necesarios, estableciendo reglas para los desarrolladores en el manejo de la información crítica.

El Área de Tecnologías de la Información deberá documentar y aplicar los principios de ingeniería para los sistemas de información, los que deberán ser monitoreados en forma periódica. También, deberá establecer y asegurar la protección del entorno en que se realizan los desarrollos de estos,

tanto internos como externos o tercerizado. Asimismo, deberá resguardar todo tipo de información cuando se realicen las pruebas funcionales, protegiendo los datos críticos y sensibles. El Ministerio deberá contar con controles para la supervisión y revisión de las aplicaciones desarrolladas por proveedores, los que deberán cumplir las cláusulas establecidas en la contratación de servicios y entregables.

4. Roles y responsabilidades

Independiente del cargo/rol que se desempeñe, del nivel jerárquico del que se goce y de la modalidad bajo la cual se esté contratado, es responsabilidad de todo el personal de este Ministerio conocer y dar debido cumplimiento a la Política de Desarrollo, asimismo, es responsabilidad de:

- **Encargado/a Área de Tecnologías de la Información**
  Velar por el cumplimiento de esta política por las personas a su cargo, creando las condiciones que sean necesaria para la protección de datos manejados por los desarrolladores del Ministerio como por desarrollos externos.
- **Encargado/a de Redes y Seguridad**
  Supervisión de lo establecido en esta política, activando controles para el resguardo de la información en los sistemas de pruebas utilizadas por los desarrolladores.
- **Encargado/a de Seguridad de la Información**
  Velar por el cumplimiento de esta política realizando revisiones periódicas.
- **Comité de Seguridad de la Información**
  Difusión de este documento, así como la constante revisión, actualización y aprobación de lo establecido en esta norma.
- **Desarrollador/a de Software**
  Apego estricto a esta política, cumpliendo los lineamientos para el resguardo de la información crítica y sensible del Ministerio.
- **Jefaturas/ Funcionarios/as Trabajadores/as**
  Conocer y dar cumplimiento a esta norma.

5. Mecanismo de difusión

Es responsabilidad del Comité de Seguridad de la Información difundir esta política, publicándose en la intranet institucional a disposición de todo el personal del Ministerio.

6. Evaluación y revisión

El tiempo de evaluación y revisión estándar para esta política, será en un plazo máximo de dos años. No obstante, podrá revisarse cuando la situación lo amerite o la autoridad así lo disponga. El/la encargado/a de seguridad de la información informará en sesión del Comité de seguridad de la información los cambios y/o actualizaciones de esta norma. El Comité de seguridad de la información la revisará, observará y aprobará esta política según la normativa vigente y lineamientos establecidos por la institución.

7. **Definiciones**

Control A.14.01.02 Aseguramiento de servicios de aplicación en redes públicas

El/la encargado/a de redes y seguridad deberá establecer los mecanismos de control que sean necesarios para suministrar los recursos de las redes de datos y de los servicios y sistemas operativos que dependan de las redes, así como preservar la integridad y confidencialidad de la información que se mueve a través de las redes de datos del Ministerio y asegurar el control de la circulación en éstas.

Se deberán tomar medidas de control para el aseguramiento de la disponibilidad de los recursos y servicios de red, así mitigar los riesgos de seguridad de la información que transita en las redes del Ministerio.

Se deberán identificar los mecanismos de seguridad, así como la clase de servicio requerido, lo que deberá ser incluido en los acuerdos de servicios de red cuando el proveedor sea externo. Asimismo, deberán identificar los servicios y puertos permitidos por el Ministerio en las redes de datos y deshabilitar o eliminar los accesos de los servicios no permitidos.

El Ministerio deberá contar con la protección necesaria entre las redes internas y externas. Se deberán determinar variables técnicas que se requieran para el acceso seguro a los servicios de red, así como protocolos de conexión de seguridad y controles para el cifrado de información que transite en las redes.

Control A.14.01.03 Protección de las transacciones de servicios de aplicación

El Ministerio deberá utilizar un canal seguro de comunicación mediante certificado SSL (Secure Socket Layer) y protocolo HTTPS para cada uno de sus portales y aplicaciones, con el fin de asegurar el envío de información desde el cliente al servidor.

Las aplicaciones deberán autenticarse con el dominio de la institución, mediante usuario/a y contraseña. Podrán tener sus propios niveles de acceso mediante el desarrollo de perfiles. Cada usuario/a deberá pertenecer a una única división, unidad y centro de costo.

Las aplicaciones podrán incorporar integraciones para el uso de firma electrónica avanzada de gobierno para el firmado de registros o documentos mediante OTP (One-Time Password). Para ello, el funcionario o colaborador deberá solicitar autorización a el/la Jefe/a de Servicio completando un registro asociado a su información institucional y un celular en donde llegará temporalmente cada código OTP para firmar desde la aplicación en uso.

Control A.14.02.01 Política de desarrollo seguro

El desarrollo seguro del Ministerio está a cargo del Área de Tecnologías de la Información y el equipo del área de desarrollo, diseño e innovación, la cual basa el desarrollo de sus proyectos en metodologías ágiles, cuyos procedimientos ofrecen instrumentos útiles para la sistematización de las actividades que dan soporte al ciclo de vida del software.

Todo requerimiento de desarrollo deberá ser ingresado de manera formal al Área de Tecnologías de la Información, en base a esto se llevará a cabo un registro en una matriz de requerimiento también llamada backlog de producto. Esta matriz deberá considerar la siguiente información:

Registro del requerimiento

- **Nº** (Identificación del requerimiento)
- **Área del sistema** (Ubicación dentro del sistema en dónde se detecta la oportunidad de mejora)
- **Originador** (Funcionario/a que especifica el requerimiento)
- **Fecha** (Fecha de la solicitud)
- **Urgencia** (Baja: Afecta a una funcionalidad o característica; Media: Afecta a un módulo; Alta: Afecta a uno o más procesos)
- **Rol** (Identificación del rol que participa en el requerimiento. En historias de usuarios/as hace referencia a "Como").
- **Necesidad** (Especificación de la necesidad de forma general. En historias de usuario/a hace referencia a "Quiero")
- **Descripción** (Descripción detallada de la Necesidad. Identificar el fin de la necesidad. En historias de usuario/a hace referencia a "Para")
- **Criterios de aceptación** (Especificar las condiciones que se deben cumplir para la aceptación del requerimiento por parte del usuario/a)
- **Estado** (Estado del requerimiento: Solicitado, Pausado, Evaluado, Aprobado, Rechazado, En Proceso, Implementado)
- **Responsable** (Funcionario/a responsable de dar solución al requerimiento)
- **Observaciones** (Incorporación de cualquier antecedente que pueda ayudar en el entendimiento del requerimiento)

Análisis de requerimiento

- **Tipo de cambio** (Corrección de error en la aplicación; Optimización o mejora en el proceso; Optimización o mejora en la funcionalidad; Cambio visual o estético; Implementación a cambios de requerimientos; Adaptación a cambios del ambiente productivo; Otro)

- **Prioridad de implementación del cambio** (Baja: Analizar la oportunidad de mejora; Media: Ejecutar la acción a corto plazo; Alta: Ejecutar la acción inmediatamente)
- **Nº de requerimiento relacionado** (Identificar requerimiento que tenga relación para definir un entregable)
- **Identificación del entregable** (Identificación única que agrupe requerimientos para un entregable. Iteración o Sprint)
- **Observaciones** (Observaciones relacionadas al requerimiento relacionado e identificación del entregable)
- **Repercusión** (Baja: No está relacionada con otras peticiones; Media: Está relacionada con 1 a 3 peticiones; Alta: Está relacionada con 3 o más peticiones)
- **Observaciones** (Observaciones relacionadas a la repercusión del requerimiento)
- **Impacto** (Bajo: Mejora de funcionalidad o característica; Medio: Mejora del módulo; Alto: Mejora del proceso)
- **Grado del cambio** (Mínimo: Algunas líneas de código; Medio: Funciones o características; Alto: Módulo nuevo)
- **Observaciones** (Observaciones relacionadas al impacto o grado del cambio)
- **Tiempo estimativo de desarrollo** (Corto plazo: 1 día; Mediano plazo: 1 a 3 días; Largo Plazo: 3 o más días)
- **Fecha estimativa de entrega** (Fecha estimativa de entrega de acuerdo con la planificación del proyecto)
- **Estado** (Estado de análisis del requerimiento: Aceptado, Rechazado)

Como medida de control para las tareas que dan respuestas al requerimiento, podrán ser desarrolladas reuniones de planificación al inicio de cada semana, reuniones diarias de control de avance y reuniones de cierre de semana para una retroalimentación del avance. Se deberá llevar a cabo un acta de reunión como registro de cada convocatoria.

Referente a la arquitectura tecnológica podrá hacer uso de lo siguiente:

- Capa de Presentación: Será la que vea, presente, comunique y capture la información de el/la usuario/a en un mínimo proceso. Esta capa se comunicará únicamente con la capa de negocio.

- Capa de Negocio: Deberán residir los programas que se ejecuten, se recibirán las peticiones de los/las usuarios/as y se enviarán respuestas tras el proceso. Esta capa se comunicará con la capa de presentación, para recibir las solicitudes y presentar los resultados, mientras que para solicitar al gestor de base de datos para almacenar o recuperar datos de él, lo hará con la capa de datos.

- Capa de Datos: Residirán los datos y será la encargada de acceder a los mismos. Estará formada por uno o más gestores de bases de datos que realizarán todo el almacenamiento de datos, recibirán solicitudes de almacenamiento o recuperación de información desde la capa de negocio.

Para el desarrollo de las aplicaciones se podrán emplear distintas plataformas según el requerimiento solicitado. El estudio de la solución deberá permitir optar por:

- Active Server Pages ASP3 – SQL Server 2000 o superior.
- Microsoft Office SharePoint Server 2007 – SQL Server 2005 o superior.
- Windows SharePoint Services 3.0 – SQL Server 2005 o superior.
- ASP.Net C# – SQL Server 2005 o superior.
- PHP – MySQL.
- Framework de Desarrollo Laravel – MySQL.
- JavaScript.

La División de Gobierno Digital podrá hacer uso de otras tecnologías adicionales o equivalentes como parte de los lineamientos internos definidos por su Jefatura.

Se deberán implantar los controles necesarios, que aseguren que las migraciones entre los ambientes de desarrollo, prueba y producción hayan sido aprobadas, así como contar son sistemas de control de versiones para administrar los cambios de los sistemas. Se deberán adoptar metodologías para la realización de pruebas de software, los que deberán contener pautas para la selección de escenarios, niveles, tipos, datos de pruebas. Además, se deberá asegurar que la plataforma, herramientas de desarrollo y los factores de cada sistema estén actualizados con las actualizaciones liberadas para las versiones que se estén utilizando. Por último, se deberán almacenar las copias de seguridad del código fuente de manera segura previniendo riesgos de pérdida de disponibilidad, confidencialidad o integridad.

Para cada desarrollo de software interno, se deberá designar una contraparte técnica para el desarrollo de aplicaciones, correspondiente al centro de responsabilidad que requiera. El funcionario designado se deberá encargar de recopilar todos los cambios necesarios detectados para el mejoramiento de sus tareas y de su equipo de trabajo con las aplicaciones y sistemas que trabajan a diario, formalizar estos requerimientos, velar por la realización de pruebas dentro de los plazos planificados y efectuar la recepción conforme de la solución realizada.

Las aplicaciones podrán incluir firmas digitalizadas de usuarios/as firmantes en documentos específicos. Para ello, deberá existir un control en donde el funcionario o colaborador involucrado especifique su firma principal y de visación autorizando la digitalización e incorporación en la aplicación que señale.

Deberán existir nomenclaturas específicas para diferenciar los ambientes de desarrollo y prueba, del ambiente productivo de portales y aplicaciones desarrolladas o disponibilizadas por la institución:

Ambiente	URL
Desarrollo	[sub dominio]-dev.[dominio].gob.cl
Beta Testing	[sub dominio]-beta.[dominio].gob.cl
Producción	[sub dominio].[dominio].gob.cl

Para los dominios.gob deberá existir una solicitud desde el/la encargado/a del Área de Tecnologías de la Información hacia el Ministerio del Interior. Deberá considerar las siguientes nomenclaturas específicas para diferenciar los ambientes de desarrollo y prueba, del ambiente productivo de portales y aplicaciones desarrolladas o disponibilizadas por la institución:

Ambiente	URL
Desarrollo	dev.[dominio].gob.cl
Beta Testing	beta.[dominio].gob.cl
Producción	[dominio].gob.cl

Control A.14.02.02 Procedimientos de control de cambios del sistema

El/la encargado/a de proyecto deberá atender, tramitar y asegurar que se efectúen los cambios en el sistema, cambios que introducen e implementan controles para la mitigación de alteraciones no autorizadas y errores, que tras su análisis se deberá implementar todos los cambios solicitados.

Cuando se ejecuten pruebas, el/la encargado/a de proyecto deberá generar los casos de prueba necesarios y deberá publicar el código fuente de su máquina local, al servidor de desarrollo. Las configuraciones deberán ser realizadas por el/la encargado/a del proyecto.

Una vez publicados los cambios en el ambiente de desarrollo, el/la encargado/a de pruebas deberá realizar la ejecución de cada caso de prueba. Si el caso de prueba no resultare exitoso y es aplicable como prueba al sistema, el/la encargado/a deberá registrar el detalle de no conformidad, para luego definir y ejecutar acciones correctivas. Si el caso de prueba no resultare exitoso, y no fuera aplicable como prueba al sistema, se deberá solicitar una redefinición del caso de prueba, para volver a ser ejecutado. Si el resultado, en el caso de prueba es exitoso, se generará un paquete para pasar a producción.

Se deberá mantener un registro de los cambios de cada aplicación o portal. Este registro deberá permitir identificar el requerimiento y generar un análisis de este, realizando una estimación de

plazo para su solución. Además, deberá considerar un control de estado, responsables y fecha de entrega.

Control A.14.02.03 Revisión técnica de las aplicaciones después de los cambios en la plataforma de operación

Cuando se deba realizar un cambio en el sistema en operación, deberá ser revisado por la persona a cargo, para asegurar que no haya impacto en el funcionamiento de las aplicaciones. Igualmente, se realizará una revisión al proceso, dando garantía de que los cambios no comprometan el proyecto o funcionalidades clave de este. Además, se deberá garantizar que cualquier cambio en el sistema operativo será informado a el/la encargado/a del proyecto antes de la implementación para efectos de tomar todos los resguardos necesarios y evitar la anulación o caída del servicio.

Control A.14.02.04 Restricciones en los cambios a los paquetes de software

Respecto de las restricciones sobre cambios en un paquete de software suministrado por un tercero que necesite ser modificada, se deberá considerar que el riesgo de aplicar los cambios no comprometa los procesos de control y de integridad existentes. La persona que se encuentre a cargo de las restricciones deberá evaluar si es necesario obtener o no el consentimiento del proveedor; y si ante un impacto, la organización es responsable por el futuro mantenimiento del software como consecuencia de los cambios.

El Área de Tecnologías de la Información, deberá conservar el software original y los cambios deberán ser aplicados a una copia claramente identificada. Todos los cambios deberán ser aprobados y documentados, de modo que puedan ser aplicados nuevamente si fuere necesario a futuras mejoras de software.

Si fuere necesaria una modificación de paquetes de software suministrados por proveedores, previa autorización del Encargado/a del Área de Tecnologías de la Información y Encargado/a de Seguridad de la Información, se deberán analizar los términos y condiciones de la licencia para determinar si las modificaciones están autorizadas.

El Área de Tecnologías de la Información, deberá hacer una evaluación del tipo de impacto que pueda producir si el Ministerio se hiciera cargo del mantenimiento.

Control A.14.02.05 Principios de ingeniería de sistema seguro

El/la encargado/a del Área de Tecnologías de la Información deberá tomar los resguardos que sean necesario para la protección de la información dentro del Ministerio, ya que cualquier vulnerabilidad puede comprometer la seguridad de la información, para lo que se deberá realizar un seguimiento de las herramientas que se utilizan para el desarrollo de sistemas. Los accesos a los sistemas deberán ser validados. En caso del intercambio de información crítica o sensible, si la

hubiere, se deberá utilizar los protocolos para el cifrado de las comunicaciones. En caso de almacenamiento, la información sensible deberá cifrarse usando algoritmos fuertes y claves robustas.

Control A.14.02.06 Entorno de desarrollo seguro

El Área de Tecnologías de la Información, deberá establecer mecanismos de protección que tengan relación con el desarrollo de sistemas, para lo cual deberá contar con:

- Controles de acceso a toda persona que no cuente con autorización para el ingreso físico a las dependencias en la cual se lleva a cabo el desarrollo, tomándose medidas establecidas en la Política de Seguridad Perimetral y de Acceso a la Información.
- Contar con los protocolos de protección que sean necesarios para el resguardo de la información, cuando el desarrollo de sistemas se encuentre en manos de terceros.
- El Ministerio deberá contar con la segregación de espacios y velar por el cumplimiento de lo establecido.
- El/la encargado/a del Área de Tecnologías de la Información deberá determinar un espacio específico para el desarrollo seguro de sistemas para las personas que cuenten con autorización para estas tareas, controlando los accesos a personas externas a la institución contando con perímetros seguros en el área de desarrollo.
- El Área de Tecnologías de la Información deberá proveer un mecanismo de control de versiones de código fuente, denominado repositorio, el cual será de acceso restringido. Esto deberá estar disponible exclusivamente dentro de la red interna de la institución y deberá ser administrado por el Área de Tecnologías de la Información. Cada proyecto de desarrollo de software deberá poseer un proyecto en este repositorio, en el cual el desarrollador deberá incorporar sus cambios al momento de realizar liberaciones para pruebas en ambientes de prueba y posteriormente producción. Por otra parte, al presentarse la necesidad de incorporar nuevos cambios en el código fuente del proyecto, deberá descargar el código fuente actualizado desde el repositorio, para contar con la última versión de este.
- El código fuente almacenado en repositorios no deberá poseer información de autenticación.
- El uso de funcionalidades o características del tipo "Impersonate" de cuentas de usuarios/as, entendiéndose el uso de la identidad de un/a usuario/a mediante privilegios elevados dentro de la aplicación, deberá ser utilizado sólo en ambientes de pruebas.
- Los servidores de bases de datos de aplicaciones en sus ambientes de desarrollo, pruebas y producción podrán ser accedidos por los desarrolladores mediante una autenticación de dominio.
- Cada desarrollador deberá tener acceso exclusivamente a las bases de datos en las cuales trabaja.
- Cada aplicación deberá considerar un/a usuario/a único/a y contraseña robusta de base de datos con los permisos necesarios para llevar a cabo las acciones requeridas. La contraseña debe ser única para cada cuenta de usuario/a de base de datos.

- Está prohibido el uso de usuario/a del tipo Super Administrador de base de datos para conectarse desde las aplicaciones en cualquiera de sus ambientes, de igual forma utilizar una autenticación de dominio personal.
- Cada aplicación deberá poseer un/a usuario/a único de base de datos el cual tendrá los privilegios necesarios para operar. En ningún caso podrá tener privilegios de Super Administrador.
- Podrán existir reportes en línea los cuales deberán tener autenticación exclusivamente de sólo lectura.

Control A.14.02.07 Desarrollo tercerizado

El/la encargado/a de redes y seguridad deberá mantener un monitoreo periódico del software abastecido externamente. Cualquier actualización que pueda modificar la configuración de éstos deberá ser verificada en un ambiente de pruebas antes de aplicarlas en el ambiente de producción. En caso de que una actualización genere un cambio drástico en la configuración del sistema, se deberá evaluar la situación para ver si es posible la continuidad del servicio sin el cambio y determinar qué problemas de seguridad conlleva la exclusión de éste.

El/la encargado/a del Área de Tecnologías de la Información deberá establecer mecanismos de control en las relaciones del Ministerio con terceros, con el fin de asegurar el resguardo de la información a la puedan tener accesos o cualquier relación con los servicios contratados cumpla con las políticas de seguridad de la información.

Deberá establecer las condiciones de conexión para los equipos en la red del Ministerio, así como, la comunicación segura, cifrado, transmisión de información desde y hacia los proveedores de servicios. También, deberá realizar las gestiones que correspondan, relacionadas con terceros que puedan acceder a los sistemas y plataformas del servicio. Además, deberá velar por el cumplimiento de los controles de software instalado y de licencia de software para extender los controles que existen en la red a equipos computacionales de terceros, cuando el proveedor, por necesidad o acuerdo, deba tener conexión de equipos a la red del Ministerio.

Los proveedores y los prestadores de servicios deberán cumplir las normas, políticas y cláusulas incluidas en los contratos con el Ministerio.

El/la encargado/a del Área de Tecnologías de la Información, deberá autorizar y dar los permisos correspondientes a los proveedores para acceder a los sistemas de información. Además, deberá verificar y monitorear la utilización de los recursos entregados al proveedor de acuerdo con las obligaciones establecidas en el contrato, como también velar por el cumplimiento de estas obligaciones.

Los/las usuarios/as que debido a sus funciones deban tener relación directa con terceros deben dar cumplimiento a esta norma para evitar la usencia intencional de contenido malicioso. Si los colaboradores del Ministerio detectan algún evento de este tipo deben contactarse inmediatamente con el Área de Tecnologías de la Información o el/la encargado/a de Seguridad de la Información.

Control A.14.02.08 Prueba de seguridad del sistema
El/la encargado/a de redes y seguridad deberá dar la debida protección a los datos de prueba entregados a los desarrolladores, internos y externos, asegurando la no filtración o mal utilización de la información crítica y sensible que se maneja en los procesos de desarrollo.

La información sensible del Ministerio que se entrega a los equipos de desarrolladores para sus pruebas deberá ser estrictamente reservada en los ambientes de producción.

Las pruebas de seguridad de los sistemas deberán ser en conformidad a la importancia y naturaleza del sistema, éstas se deberán realizar con las herramientas proporcionadas por el Área de Tecnologías de la Información, estas son las pruebas de vulnerabilidad de los sistemas.

Control A.14.02.09 Prueba de aprobación del sistema
El Área de Tecnologías de la Información, durante la etapa de desarrollo deberá realizar pruebas de la funcionalidad y aplicar metodologías y definir programas para efectuar pruebas de aceptación del sistema en relación con la seguridad de éste, estableciendo programas de prueba seguros y confiables.

Se deberán hacer pruebas de aseguramiento que cumplan los protocolos de seguridad en el ambiente de prueba y producción, aprobando los pasos, actualizaciones, funcionalidades o nuevas versiones desarrolladas tanto internamente como por externos o terceros que hayan sido contratados por el Ministerio.

El entorno en que se realizan las pruebas deberá resguardar la información, no permitiendo vulnerabilidades de los sistemas que puedan afectar tanto al sistema como a la información contenida en ellos.

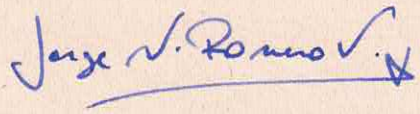
Control A.14.03.01 Protección de datos de prueba
El/la encargado/a del Área de Tecnologías de la Información deberá asegurar la protección y aplicar los controles necesarios para el resguardo de los datos de prueba. No se podrá utilizar información crítica o sensible como datos de pruebas, de lo contrario deberá solicitar los permisos que correspondan para la utilización de estos datos, los que deberán ser tratados en ambientes debidamente controlados.

Se deberá contar con autorización por cada proceso de prueba.

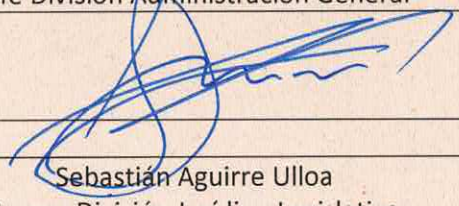
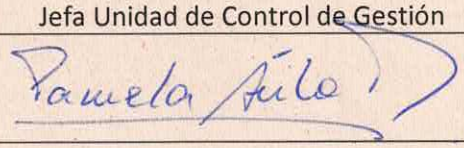
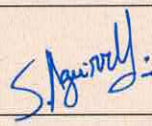
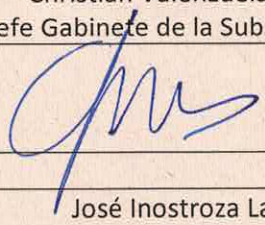
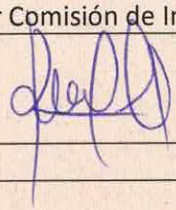
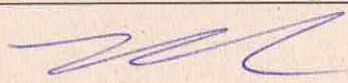
Toda información deberá ser eliminada una vez finalizada la prueba o cuando ya no sea necesaria su utilización.

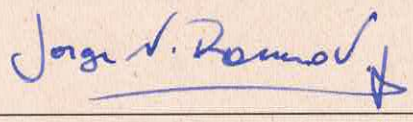
Para la protección de la información en los ambientes de prueba se aplicará lo establecido en la Política de acceso a la Información.

8. Control

Elaborado por: Jorge Romero Vargas

Fecha: 11-08-2023

Comité de Seguridad de la Información, Ministerio Secretaría General de la Presidencia

Samir Toro Garrido Jefe División Administración General	Pamela Ávila Rubio Jefa Unidad de Control de Gestión
	
Sebastián Aguirre Ulloa Asesor División Jurídico-Legislativa	Christian Valenzuela Lorca Jefe Gabinete de la Subsecretaria
	
Fabiola Vidal Oyarzún Asesor Comisión de Integridad y Transparencia	José Inostroza Lara Jefe División de Gobierno Digital
	

Jorge Romero Vargas Oficial de Seguridad de la Información Encargado Área de Tecnologías de la Información

Fecha: 11-08-2023