# ANEXO UNICO
# PROTOCOLO DE CIBERSEGURIDAD

## Capítulo 1
## Política de Control de Acceso

### 1.0 OBJETIVO

Garantizar que los controles de acceso estén implementados y cumplan con las políticas, estándares y procedimientos de seguridad de TI.

### 2.0 POLÍTICA

1. ADMINISTRACIÓN DE CUENTAS
   El Departamento de TI deberá:

   a. Identificar y seleccionar los siguientes tipos de cuentas de los sistemas de información para respaldar los objetivos organizacionales y las funciones operativas: individual, compartida, grupal, de sistema, invitada/anónima, de emergencia, desarrollador/fabricante/proveedor, temporal y de servicio.

   b. Asignar administradores de cuentas para las cuentas de los sistemas de información.

   c. Establecer condiciones para la pertenencia a grupos y roles.

   d. Especificar los usuarios autorizados de los sistemas de información, la pertenencia a grupos y roles, y las autorizaciones de acceso (es decir, privilegios) y otros atributos (según sea necesario) para cada cuenta.

   e. Requerir aprobaciones por parte de los propietarios de los sistemas de información para creación de cuentas en los mismos.

   f. Crear, habilitar, modificar, deshabilitar y eliminar cuentas de los sistemas de información de acuerdo con los procedimientos aprobados.

   g. Monitorear el uso de las cuentas de los sistemas de información.

h. Notificar a los administradores de cuentas cuando las cuentas ya no sean necesarias, cuando los usuarios sean eliminados o transferidos, y cuando se modifique el uso de los sistemas de información.

i. Autorizar el acceso a los sistemas de información a través de una autorización de acceso válida o uso previsto para los sistemas.

j. Revisar las cuentas de los sistemas de información para verificar el cumplimiento de los requisitos de administración de cuentas mensualmente.

k. Establecer un proceso para volver a emitir credenciales de cuentas compartidas/grupales (si se implementan) cuando se eliminen personas del grupo.

l. Emplear mecanismos automatizados para apoyar la gestión de cuentas de los sistemas de información.

m. Asegurar que los sistemas de información desactiven automáticamente las cuentas temporales y de emergencia después de su uso.

n. Asegurar que los sistemas de información deshabiliten automáticamente las cuentas inactivas después de treinta días.

o. Asegurar que los sistemas de información auditen automáticamente las acciones de creación, modificación, habilitación, deshabilitación y eliminación de cuentas, y notifique al personal de TI correspondiente.

2. APLICACIÓN DEL ACCESO
   El Departamento de TI deberá:

   a. Asegurar que los sistemas de información hagan cumplir las autorizaciones aprobadas para el acceso lógico a la información y los recursos de los sistemas de acuerdo con las políticas de control de acceso aplicables.

3. APLICACIÓN DEL FLUJO DE INFORMACIÓN
   El Departamento de TI deberá:

   a. Garantizar que los sistemas de información hagan cumplir las autorizaciones aprobadas para controlar el flujo de información dentro de los sistemas y entre sistemas interconectados según la política aplicable.

4. SEPARACIÓN DE TAREAS
   El Departamento de TI deberá:
   a. Separar los deberes de los individuos según sea necesario, para prevenir actividades malévolas sin colusión.

b. Documentar la separación de deberes de las personas.

c. Definir autorizaciones de acceso a los sistemas de información para soportar la separación de funciones.

5. PRIVILEGIOS MÍNIMOS
   El Departamento de TI deberá:

   a. Emplear el principio de menor privilegio, permitiendo solo accesos autorizados para los usuarios (o procesos que actúan en nombre de los usuarios) que sean necesarios para realizar las tareas asignadas de acuerdo con los objetivos organizacionales y las funciones operativas.

   b. Autorizar explícitamente el acceso al hardware y software que controla el acceso a los sistemas y reglas de filtrado de enrutadores/firewalls, sistemas de gestión de claves criptográficas, parámetros de configuración de servicios de seguridad y listas de control de acceso.

   c. Requerir que los usuarios de cuentas o roles de los sistemas de información con acceso a funciones de seguridad definidas por la Repartición o información relevante para la seguridad utilicen cuentas o roles sin privilegios al acceder a funciones que no son de seguridad.

   d. Restringir las cuentas privilegiadas en los sistemas de información a personal o roles definidos por la Repartición.

   e. Asegurar que los sistemas de información auditen la ejecución de funciones privilegiadas.

   f. Asegurar que los sistemas de información impidan que los usuarios sin privilegios ejecuten funciones privilegiadas que incluyan deshabilitar, eludir o alterar las salvaguardias/contramedidas de seguridad implementadas.

6. INTENTOS DE INICIO DE SESIÓN FALLIDOS
   El Departamento de TI deberá garantizar que los sistemas de información:

   a. Apliquen un límite de intentos consecutivos de inicio de sesión no válidos por parte de un usuario durante una frecuencia definida por la entidad.

   b. Bloqueen la cuenta/nodo automáticamente durante 48 horas o hasta que un administrador lo libere cuando se excede el número máximo de intentos fallidos.

7. NOTIFICACIÓN DE USO DE LOS SISTEMAS
   El Departamento de TI deberá garantizar que los sistemas de información:

a. Provean a los usuarios un mensaje aprobado o banner de notificación de uso de los sistemas, antes de otorgarles acceso al sistema, que proporcione avisos de privacidad y seguridad consistentes con las leyes, directivas, políticas, regulaciones, estándares y guías estatales y federales aplicables, informando que:

    i. Los usuarios están accediendo a un sistema de información de Gobierno de Jujuy.

    ii. El uso de los sistemas de información puede ser monitoreado, registrado y sujeto a auditoría.

    iii. El uso no autorizado de los sistemas de información está prohibido y sujeto a sanciones penales y civiles.

    iv. El uso de los sistemas de información indica consentimiento al seguimiento y registro.

    v. No hay derechos a la privacidad.

b. Mantengan el mensaje de notificación o banner en la pantalla hasta que los usuarios acepten las condiciones de uso y tomen acciones explícitas para iniciar sesión o acceder a los sistemas de información.

c. Para sistemas de acceso público, el Departamento de TI deberá garantizar que los sistemas de información:

    i. Provean información de uso, antes de otorgar acceso adicional.

    ii. Provean referencias, si las hay, a monitoreo, registro o auditoría que sean consistentes con las adaptaciones de privacidad para dichos sistemas que generalmente prohíben esas actividades.

    iii. Incluyan una descripción de los usos autorizados de los sistemas.

8. BLOQUEO DE SESIÓN
   El Departamento de TI deberá garantizar que los sistemas de información:

   a. Eviten un mayor acceso al sistema, iniciando un bloqueo de sesión después de 30 días de inactividad o al recibir una solicitud de un usuario.

   b. Conserven el bloqueo de la sesión hasta que el usuario restablezca el acceso, utilizando los procedimientos de identificación y autenticación establecidos.

   c. Oculten, mediante el bloqueo de sesión, información previamente visible en la pantalla, con una imagen visible públicamente.

9. TERMINACIÓN DE LA SESIÓN
   El Departamento de TI deberá:

   a. Asegurar que los sistemas de información finalicen automáticamente la sesión de un usuario después de frecuencia definida por la entidad.

10. ACCIONES PERMITIDAS SIN IDENTIFICACIÓN NI AUTENTICACIÓN
    El Departamento de TI deberá:

    a. Identificar las acciones de usuario que se puedan realizar en los sistemas de información sin identificación o autenticación, que sean consistentes con los objetivos organizacionales y funciones operativas.

    b. Documentar y proporcionar fundamentos de respaldo en el plan de seguridad de los sistemas de información, las acciones de usuario que no requieran identificación o autenticación.

11. ACCESO REMOTO
    El Departamento de TI deberá:

    a. Establecer y documentar restricciones de uso, requisitos de configuración/conexión y lineamientos de implementación para cada tipo de acceso remoto permitido.

    b. Autorizar el acceso remoto a los sistemas de información, previamente a permitir dichas conexiones.

    c. Asegurar que los sistemas de información monitoreen y controlen los métodos de acceso remoto.

    d. Asegurar que los sistemas de información implementen mecanismos criptográficos para proteger la confidencialidad e integridad de las sesiones de acceso remoto.

    e. Asegurar que los sistemas de información canalicen todos los accesos remotos a través de número definido por la entidad puntos de control administrados de acceso a la red, para reducir el riesgo de ataques externos.

    f. Autorizar la ejecución de comandos privilegiados y el acceso a información relevante para la seguridad, mediante acceso remoto, únicamente para necesidades definidas por la Repartición.

    g. Documentar la justificación de dicho acceso en el plan de seguridad de los sistemas de información.

12. ACCESO INALÁMBRICO

El Departamento de TI deberá:

a. Establecer restricciones de uso, requisitos de configuración/conexión y guías de implementación para el acceso inalámbrico.

b. Autorizar el acceso inalámbrico a los sistemas de información, previamente a permitir dichas conexiones.

c. Asegurar que los sistemas de información protejan el acceso inalámbrico al sistema mediante la autenticación de usuarios y dispositivos y cifrado.

13. CONTROL DE ACCESO PARA DISPOSITIVOS MÓVILES

El Departamento de TI deberá:

a. Establecer restricciones de uso, requisitos de configuración, requisitos de conexión y guías de implementación para dispositivos móviles controlados por la organización.

b. Autorizar la conexión de dispositivos móviles a los sistemas de información organizacionales.

c. Emplear cifrado de dispositivo completo o cifrado de contenedores para proteger la confidencialidad y la integridad de la información en los dispositivos aprobados.

14. USO DE SISTEMAS DE INFORMACIÓN EXTERNOS

El Departamento de TI deberá:

a. Establecer términos y condiciones consistentes con cualquier organización con la que exista una relación de confianza establecida, que posean, operen y/o mantengan sistemas de información externos, permitiendo a las personas autorizadas:

    i. Acceder a los sistemas de información desde sistemas de información externos.

    ii. Procesar, almacenar o transmitir información controlada por la organización, utilizando sistemas de información externos.

b. Permitir que las personas autorizadas utilicen un sistema de información externo para acceder a los sistemas de información o para procesar, almacenar o transmitir información controlada por la organización, solo cuando la organización:

i. Verifique la implementación de los controles de seguridad requeridos en los sistemas externos, según lo especificado en la política y el plan de seguridad de la información de la organización.

ii. Conserve los acuerdos de procesamiento o conexión de los sistemas de información aprobados con la entidad organizacional que aloja los sistemas de información externos.

15. EL INTERCAMBIO DE INFORMACIÓN
El Departamento de TI deberá:

a. Facilitar el intercambio de información, permitiendo a los usuarios autorizados determinar si las autorizaciones de acceso asignadas al socio compartido, coinciden con las restricciones de acceso a la información para circunstancias de intercambio de información definidas por la Repartición donde se requiere la discreción del usuario.

b. Emplear mecanismos automatizados o procesos manuales definidos por la Repartición para ayudar a los usuarios a tomar decisiones de colaboración/intercambio de información.

16. CONTENIDO PÚBLICAMENTE ACCESIBLE
El Departamento de TI deberá:

a. Designar personas autorizadas para publicar información en un sistema de información de acceso público.

b. Capacitar a las personas autorizadas para garantizar que la información de acceso público no contenga información no pública.

c. Revisar el contenido propuesto, antes de publicarlo en los sistemas de información de acceso público, para garantizar que no se incluya información no pública.

d. Revisar el contenido de los sistemas de información de acceso público en busca de información no pública frecuencia definida por la Repartición y eliminar dicha información, si la descubre.

## 3.0 CUMPLIMIENTO

Los empleados que incumplan esta política pueden estar sujetos a medidas disciplinarias que pueden incluir el sumario, así como sanciones civiles y penales. Los no empleados, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

## 4.0 EXCEPCIONES DE POLÍTICA

Las solicitudes de excepciones a esta política serán revisadas por el Director de Ciberseguridad (DC) y la Secretaría de Innovación Pública (SIP). Los departamentos que soliciten excepciones deberán proporcionar dichas solicitudes a la SIP. La solicitud debe indicar específicamente el alcance de la excepción junto con la justificación para otorgar la excepción, el posible impacto o riesgo asociado al otorgar la excepción, las medidas de mitigación de riesgos que debe tomar el Departamento de TI, iniciativas, acciones y un cronograma para lograr el nivel mínimo de cumplimiento de las políticas aquí establecidas. La SIP revisará dichas solicitudes y concederá al departamento solicitante.

## 5.0 DEPARTAMENTO RESPONSABLE

Oficina principal de información y propietarios de sistemas de información.

## 6.0 HISTORIAL DE REVISIONES

| Fecha | Descripción de Cambio | Crítico |
|---|---|---|
| 12-06-2024 | Draft final del documento | Alejandro Castro<br>Pablo Zalazar |

REFERENCIA

Publicaciones especiales (SP) del Instituto Nacional de Estándares y Tecnología (NIST): NIST SP 800-53a - Control de acceso (AC), NIST SP 800-12, NIST 800-46, NIST SP 800-48, NIST SP 800-77, NIST SP 800-94, NIST SP 800-97, NIST SP 800-100, NIST SP 800-113, NIST SP 800-114, NIST SP 800-121, NIST SP 800-124, NIST SP 800-164;
Estándares federales de procesamiento de información ( FIPS) 199 del NIST

# Capitulo 2

# Estándar de gestión de cuentas/control de acceso

## 1.0 Propósito y Beneficios

El propósito de esta norma es establecer las reglas y procesos para crear, mantener y controlar el acceso de una identidad digital (cuenta) a las aplicaciones y recursos de una organización, como medio para proteger sus sistemas de información.

## 2.0 Alcance

Este estándar cubre todos los sistemas desarrollados por o en nombre de la entidad que requieren acceso autenticado. Esto incluye todos los sistemas de desarrollo, pruebas, control de calidad, producción y otros sistemas ad hoc.

## 3.0 Declaración de información

La gestión de cuentas y el control de acceso incluyen el proceso de solicitar, crear, emitir, modificar y deshabilitar cuentas de usuario; habilitar y deshabilitar el acceso a recursos y aplicaciones; establecer condiciones para la pertenencia a grupos y roles; seguimiento de cuentas y sus respectivas autorizaciones de acceso; y gestionar estas funciones.

### 3.1 Funciones de gestión de cuentas/control de acceso

La gestión de cuentas y el control de acceso requieren que los roles de propietario de la información, administrador general de cuentas y, opcionalmente, administradores de cuentas, estén definidos y asignados para cada recurso y aplicación. Se debe documentar y mantener una lista de usuarios autorizados en estos roles. Las tareas y responsabilidades asociadas a cada función se describen a continuación. Cada rol puede pertenecer a una o más personas según la aplicación. En algunos casos, a un solo individuo o grupo se le puede asignar más de uno de estos roles.

a. **Propietario de la información:** Son personas en el nivel gerencial dentro de una entidad, que:
    1. Delegan funciones operativas a los administradores generales de cuentas, para garantizar que se proporcione el nivel adecuado de acceso a la información. La delegación puede realizarse a usuarios individuales, grupos y/o terceros (por ejemplo, otra entidad).
    2. Definen roles y grupos, así como el nivel correspondiente de acceso a los recursos para ese rol o grupo.
    3. Determinan quién debería tener acceso.
    4. Determinan el nivel de garantía de las identidades para el acceso a aplicación y/o los datos. (ver estándar de autenticación tokens)

5. Revisan que las cuentas y los controles de acceso sean proporcionales a la función operativa general y que los permisos asociados se hayan asignado adecuadamente, como mínimo, anualmente.
6. Exigen a las unidades organizativas o reparticiones, con acceso a recursos protegidos, que notifiquen a los administradores de cuentas cuando las cuentas ya no sean necesarias, como cuando los usuarios son dados de baja o transferidos y cuando cambian los requisitos de acceso individual.

**b. Administrador general de cuentas:** Gestiona las cuentas. Es el custodio delegado de los datos protegidos. El administrador general de cuentas:

1. Mantiene niveles apropiados de comunicación con los propietarios de la información, para determinar el nivel o grado de acceso otorgado a un individuo.
2. Determina las especificaciones técnicas necesarias para establecer privilegios de acceso.
3. Delega funciones de gestión de cuentas a administradores de cuentas.
4. Crea y mantiene los procedimientos utilizados en la gestión de cuentas.
5. Realiza todas las tareas de administradores de cuentas según sea necesario.

**c. Administradores de cuentas:** Son un subconjunto opcional de la función de administrador general de cuentas. No determinan procedimientos. El administrador general de cuentas les asigna los derechos y/o responsabilidades del sistema. Todas las responsabilidades de los administradores de cuentas están contenidas en la función de administrador general de cuentas, en caso de que no existan administradores de cuentas. Se podrá asignar un subconjunto de funciones del administrador general de cuentas, según corresponda. Por ejemplo, es posible que exista una función para restablecer contraseñas únicamente para los empleados de la mesa de entrada. Además, algunas de estas responsabilidades pueden permanecer en el administrador general de cuentas, si éste determina que es necesario. Para la gestión de cuentas, el administrador podrá:

1. Mantener toda la información necesaria que respalde las actividades de administración de cuentas, incluidas las solicitudes y aprobaciones de administración de cuentas.
2. Inscribir nuevos usuarios.
3. Activar/desactivar cuentas de usuario.
4. Crear y mantener roles y grupos de usuarios.
5. Asignar derechos y privilegios a un usuario o grupo.
6. Recopilar datos para revisar periódicamente las cuentas de usuario y sus derechos asociados.
7. Asignar nuevos tokens de autenticación (por ejemplo, restablecimiento de contraseñas).

**d. Administrador de permisos:** Son un subconjunto opcional de la función de administrador de cuentas. Los permisos y/o responsabilidades les son definidos por el titular de la información (o sus delegados) y generalmente incluyen:

1. Asignar derechos y privilegios a un usuario, grupo o rol.

2. Recopilar datos para revisar periódicamente las cuentas de usuario y sus permisos asociados.
3. Mantener toda la información necesaria que respalde las actividades de administración de cuentas, incluidas las solicitudes y aprobaciones de administración de cuentas.

### 3.2 Tipos de cuentas

Los tipos de cuentas incluyen: individual, privilegiada, de servicio, compartida, invitada/anónima, de emergencia y temporal. Todos los tipos de cuentas deben cumplir con todas las reglas aplicables según lo definido en el Estándar de tokens de autenticación.

**a. Cuentas individuales:** una cuenta individual es una cuenta única, emitida para un solo usuario. La cuenta permite al usuario autenticarse en sistemas con una identidad digital. Después de autenticar a un usuario, se le autoriza o se le niega el acceso al sistema, según los permisos que se le asignan directa o indirectamente (permisos heredados).

**b. Cuentas privilegiadas:** una cuenta privilegiada es una cuenta que proporciona mayor acceso y requiere autorización adicional, por ejemplo, cuentas de administradores de red, de sistema o de seguridad. Solo se puede proporcionar una cuenta privilegiada a agentes y funcionarios que la requieran para cumplir con sus débitos laborales. El uso de cuentas privilegiadas debe cumplir con el principio de privilegio mínimo. El acceso se restringirá únicamente a aquellos programas o procesos específicamente necesarios para realizar tareas operativas autorizadas y nada más. Hay dos tipos de cuentas privilegiadas: cuentas administrativas y cuentas privilegiadas predeterminadas.

1. **Cuentas administrativas:** Cuentas concedidas a un usuario que le otorgan el derecho de modificar la configuración del sistema operativo o de la plataforma, o aquellas que permiten modificaciones de otras cuentas. Estas cuentas deben:
    i. Estar en un nivel de garantía de identidad acorde con los recursos protegidos a los que acceden.
    ii. No poseer un ID de usuario que proporcione indicios acerca del nivel de privilegio del mismo, por ejemplo, supervisor, gerente, administrador o cualquier tipo aplicable.
    iii. Ser identificables internamente como cuentas administrativas según una convención de nomenclatura estandarizada.
    iv. Ser revocadas de acuerdo con los requisitos organizacionales.

2. **Cuentas privilegiadas predeterminadas:** las cuentas privilegiadas predeterminadas (por ejemplo, administrador o root) se proporcionan con un sistema en particular y no se pueden eliminar sin afectar la funcionalidad del sistema. Las cuentas privilegiadas predeterminadas deben:

i. Deshabilitarse si no está en uso o cambiarse de nombre si es técnicamente posible.
ii. Utilizarse únicamente para la instalación inicial del sistema o para realizar tareas de mantenimiento. Cuando sea técnicamente posible, deben emitirse alertas al personal apropiado, cuando éstas sean utilizadas para iniciar sesión.
iii. Poseer una contraseña que no sea la predeterminada o inicialmente asignada por el sistema.
iv. Poseer una contraseña conocida o accesible por al menos dos personas dentro de la organización.

**c. Cuentas de servicio:** una cuenta de servicio no está destinada a ser otorgada a un usuario, sino que se proporciona para la ejecución de un proceso, usualmente automatizado. Debe usarse en situaciones tales como permitir que un sistema ejecute trabajos y servicios independientemente de la interacción del usuario. Las cuentas de servicio deben:

1. Tener un propietario asignado, responsable de documentar y administrar la cuenta.
2. Restringirse a dispositivos y horarios específicos cuando sea posible.
3. Ser gestionadas, de forma tal, que su utilización no se realice de manera interactiva por un usuario, para ningún propósito que no sea la instalación inicial del sistema o, si es absolutamente necesario, para la resolución de problemas o mantenimiento del sistema. Siempre que sea técnicamente posible, los administradores deben aprovechar mecanismos de “cambio de usuario” o “ejecutar como” para lanzar procesos mediante cuentas de servicio.
4. Utilizarse únicamente para propósitos circunscriptos a su alcance inicial.
5. Ser identificables internamente, cuando sea posible, como cuentas de servicio según una convención de nomenclatura estandarizada.
6. Estar exentas de cronogramas estandarizados y/o forzados de rotación de credenciales. Sin embargo, si un integrante de la organización, con conocimiento de dicha contraseña, abandonara la entidad, dichas credenciales deberán ser cambiadas inmediatamente.
7. Poseer una contraseña conocida o accesible por al menos dos personas dentro de la organización.

**d. Cuentas compartidas:** una cuenta compartida es cualquier cuenta en la que más de una persona conoce la contraseña y/o utiliza el mismo token de autenticación. El uso de cuentas compartidas solo se permite cuando existe una limitación del sistema o de la operación que impide el uso de cuentas individuales. Estos casos deben ser documentados por el propietario de la información y revisados por el responsable de seguridad designado. Se deben implementar controles compensatorios adicionales para confirmar que se mantiene la rendición de cuentas. Las cuentas compartidas deben:

1. Restablecer los tokens (por ejemplo, la contraseña) cuando alguno de sus usuarios ya no necesite acceso, o de otro modo de acuerdo con el Estándar

de Tokens de Autenticación.
2. Restringirse a dispositivos y horarios específicos, cuando sea posible.
3. Siempre que sea técnicamente posible, hacer que sus usuarios inicien sesión en el sistema con sus cuentas individuales y "cambien de usuario" (SU) o "ejecuten como" la cuenta compartida.
4. Contar con permisos estrictamente limitados y acceso solo a los sistemas requeridos.

**e. Cuentas predeterminadas sin privilegios:** la cuenta predeterminada sin privilegios (invitado o usuario anónimo) es una cuenta para personas que no tienen cuentas individuales. Un ejemplo de dónde esto podría ser necesario es en una red Wi-Fi pública. Este tipo de cuentas deben:

1. Desactivarse hasta que sea necesario.
2. Poseer restricciones y permisos limitados.
3. Permitirse únicamente luego de una evaluación de riesgos.
4. Tener controles compensatorios que incluyan acceso restringido a la red.
5. Tener asignada una contraseña que el usuario no pueda cambiar, pero que se actualice por un administrador, como mínimo, mensualmente.
6. Prohibir sean delegadas a otra cuenta.
7. Mantener un registro de usuarios a quienes se les proporciona la contraseña.

**f. Cuentas de emergencia:** Las cuentas de emergencia están destinadas a un uso de corto plazo e incluyen restricciones de creación, punto de origen y uso (por ejemplo, hora del día, día de la semana). El Oficial de Seguridad de la Información (ISO)/representante de seguridad designado, puede establecer cuentas de emergencia en respuesta a situaciones de crisis. Por lo tanto, la activación de emergencia de las cuentas, pueden eludir los procesos normales de autorización de las mismas. Las cuentas de emergencia deben desactivarse automáticamente después de 24 horas.

**g. Cuentas temporales:** Las cuentas temporales están destinadas a un uso de corto plazo e incluyen restricciones de creación, punto de origen, uso (por ejemplo, hora del día, día de la semana) y deben tener fechas pautadas de inicio y finalización para su desactivación. Una Unidad de Organización puede establecer cuentas temporales como parte de los procedimientos normales de activación de cuentas, cuando existe la necesidad de cuentas de corto plazo y no existe la exigencia de inmediatez en la activación de la misma. Estas cuentas deben tener permisos y accesos estrictamente limitados a los sistemas requeridos.

### 3.3 Funciones de gestión de cuentas y control de acceso

En caso de ser posible, se deben emplear mecanismos automatizados para monitorear el uso y la gestión de las cuentas. Estos mecanismos deben permitir el monitoreo del uso y emitir notificaciones, en caso de uso atípico de las mismas. Los umbrales para las alertas deben establecerse según la importancia del sistema o el nivel de seguridad de la cuenta.

Se debe notificar al personal que desempeña las funciones apropiadas de administración de cuentas/control de acceso, cuando se realicen actividades de administración de cuentas, como, por ejemplo, cuando las cuentas ya no sean necesarias, los usuarios sean eliminados, dados de baja o transferidos. Estas actividades deberían automatizarse, siempre que sea técnicamente posible.

Dentro de los sistemas, deben existir políticas de control de acceso automatizadas, siempre que sea posible, que hagan cumplir las autorizaciones aprobadas para la información y los recursos del sistema. Estas políticas de control de acceso podrán basarse en identidad, rol o atributos.

De forma predeterminada, nadie debe contar con acceso a los sistemas de información, a menos que esté autorizado.

El Nivel de Garantía de Identidad (NGI) de un sistema, determina el grado de certeza requerido al verificar la identidad de un usuario. La siguiente tabla describe el nivel de confianza asociado con cada NGI:

| ***Nivel de garantía de identidad*** | ***Descripción*** |
|---|---|
| **1** | **Confianza baja o nula en la validez de la identidad afirmada** |
| **2** | **Confianza en la validez de la identidad afirmada.** |
| **3** | **Alta confianza en la validez de la identidad afirmada.** |

La Tabla 1 refleja los estándares para la gestión de cuentas en cada nivel de aseguramiento.

**Tabla 1: Estándares de gestión de cuentas por nivel de garantía de identidad**

| | Niveles de garantía de identidad | | |
|---|---|---|---|
| Categoría | 1 | 2 | 3 |
| Cuenta desactivada automáticamente después de *x* días de inactividad | 1096 | 90 | 90 |
| Enviar notificación *x* días antes de que la cuenta se deshabilite | 30 | 30 | 14 |
| Cuenta bloqueada después de *x* número de intentos fallidos consecutivos de inicio de sesión | 10 | 5 | 3 |
| La creación de una cuenta requiere un atributo autorizado que vincule al usuario a su cuenta. Por ejemplo, podría ser una identificación de empleado, una identificación de licencia de conducir, una identificación fiscal o una dirección de correo electrónico individual única. | No | Sí | Sí |

| | Niveles de garantía de identidad | | |
|---|---|---|---|
| Categoría | 1 | 2 | 3 |
| Se enviará una notificación por correo electrónico al usuario para los siguientes eventos:<br>• Cambio de token (contraseña, token de conocimiento pre-registrado, información del token fuera de banda (OOB))<br>• Cuenta inhabilitada debido a intentos no válidos<br>• Se ha emitido una identificación de usuario (UID) olvidada<br>• Cambio de atributo de cuenta (por ejemplo, cambio de nombre)<br>• Reactivación de cuenta | Si se sabe | Sí | Sí |
| Funcionalidad de autoservicio permitida | Sí | Sí | No |

Para todos los niveles de garantía, se debe cumplir lo siguiente.

**a. Creación de cuentas nuevas:** para crear una cuenta, debe haber una autorización de acceso válida basada en una justificación operativa aprobada y debe realizarse una solicitud formal para crear la cuenta.

**b. Modificación de los atributos de la cuenta (es decir, cambiar los nombres de los usuarios, datos demográficos, etc.):** Las modificaciones solo deben ser realizadas por el usuario autenticado o un administrador de cuentas autorizado.

**c. Habilitación de acceso:** El acceso se otorga, según el principio de privilegio mínimo, con una autorización de acceso válida.

**d. Modificación de acceso:** Las modificaciones de acceso deben incluir una autorización válida. Cuando haya un cambio de rol, función o cargo (sin incluir desvinculación), el acceso debe revisarse inmediatamente y se suspende/elimina cuando ya no es necesario.

**e. Deshabilitar cuentas/eliminar acceso:**

1. **Basado en eventos/riesgos (desactivación administrativa):** cuando una cuenta presenta o tiene el potencial de representar un riesgo significativo, la cuenta se deshabilita y/o los atributos de acceso se eliminan al descubrir el riesgo. Es esencial una estrecha coordinación entre los propietarios de la información, los administradores/responsables de cuentas, las partes interesadas legales, de respuesta a incidentes y los responsables de recursos humanos para ejecutar oportunamente la eliminación o restricción del acceso de los usuarios. Los usuarios que representan un riesgo significativo para las

organizaciones incluyen personas para quienes evidencia o inteligencia confiable indican la intención de utilizar el acceso autorizado a los sistemas de información para causar daño o a través de quienes los adversarios causarán daño. El daño incluye posibles impactos adversos a las operaciones y activos de la repartición, a los individuos y a otras organizaciones. Se requiere un identificador de cuenta para identificar estas cuentas y evitar una reactivación inapropiada de la cuenta/acceso. Volver a habilitar la cuenta requiere la aprobación explícita de la repartición. No se pueden utilizar mecanismos de autoservicio para volver a habilitar la cuenta.

2. **Desactivación tras la desvinculación**: todas las cuentas de usuario (incluidas las privilegiadas) deben desactivarse inmediatamente después de la desvinculación. Además, las credenciales deben revocarse de acuerdo con los requisitos de la repartición y se deben eliminar los atributos de acceso. No se podrán utilizar mecanismos de autogestión para volver a habilitar la cuenta o sus permisos.

3. **Deshabilitación por inactividad:** cuando una cuenta se deshabilita debido a inactividad, los atributos de acceso pueden permanecer sin cambios si el propietario de la información lo considera apropiado. La reactivación será a través de su respectiva vía administrativa.

**f. Revisión de cuentas y acceso:**

1. Los propietarios de la información deben revisar todas las cuentas anualmente (como mínimo) para determinar si todavía son necesarias.
2. El acceso a cuentas privilegiadas debe revisarse cada seis meses (como mínimo) para determinar si todavía son necesarias o no.
3. Los propietarios de la información deben revisar las autorizaciones de cuentas y/o las asignaciones de acceso de los usuarios anualmente (como mínimo) para determinar si aún se necesita todo el acceso.
4. Las cuentas o registros de la cuenta deben archivarse después de 5 años de inactividad o después de que se cumplan propósitos de auditoría específicos.

**g. Desbloqueo de cuentas de usuario:** Para que un administrador o técnico de soporte informático desbloquee una cuenta para un usuario, el usuario debe ser examinado mediante tokens de conocimiento pre-registrados según el Estándar de Autenticación Tokens.

**h. Procedimientos de inicio de sesión seguro:** cuando sea técnicamente posible, el acceso debe controlarse mediante procedimientos de inicio de sesión seguro de la siguiente manera:

1. No debe mostrar los tokens (por ejemplo, contraseña, PIN) que se ingresan.

2. Debe mostrar la siguiente información al completar un inicio de sesión exitoso:
   i. Fecha y hora del inicio de sesión exitoso anterior; y

ii. Detalles de cualquier intento fallido de inicio de sesión desde el último inicio de sesión exitoso.

i. **Bloqueo de inactividad de sesión:** las sesiones deben bloquearse después de un período máximo de inactividad de 15 minutos. Los bloqueos de inactividad de sesión son acciones temporales que se toman cuando los usuarios dejan de trabajar y se alejan de su entorno inmediato, pero no quieren cerrar sesión debido a la naturaleza temporal de sus ausencias. Los usuarios deben volver a autenticarse para desbloquear la sesión.

j. **Tiempo de espera de sesión activas:** las sesiones deben finalizar automáticamente después de 18 horas o después de condiciones "predefinidas", como respuestas específicas a ciertos tipos de incidentes.

k. **Registro/Auditoría/Monitoreo:** toda la actividad de la cuenta debe registrarse y auditarse de acuerdo con el Estándar de Registro de Seguridad. La capacidad de modificar o eliminar registros de auditoría debe evitarse tanto como sea posible y limitarse a un conjunto específico de cuentas privilegiadas. Cualquier modificación de los atributos de acceso debe registrarse y rastrearse hasta un solo individuo.

## 4.0 Cumplimiento

Los empleados que incumplan esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y administrativas. Los no empleados, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

## 5.0 Excepciones de Política

Las solicitudes de excepciones a esta política serán revisadas por el Director de Ciberseguridad (DC) y la Secretaría de Innovación Pública (SIP) o Encargado de Información. Los departamentos que soliciten excepciones deberán proporcionarle dichas solicitudes. La solicitud debe indicar específicamente el alcance de la excepción junto con la justificación para otorgar la excepción, el posible impacto o riesgo asociado al otorgar la excepción, las medidas de mitigación de riesgos que debe tomar el Departamento de TI, iniciativas, acciones y un cronograma para lograr el nivel mínimo de cumplimiento de las políticas aquí establecidas. El DC revisará dichas solicitudes y concederá al departamento solicitante dejando asentada la excepción.

## 6.0 Departamento Responsable

Oficina principal de información y propietarios de sistemas de información.

## 7.0 Historial de revisiones

| Fecha | Descripción de Cambio | Revisado por |
|---|---|---|
| 27-05-2024 | Draft final del documento | Alejandro Castro<br>Pablo Zalazar |
| 29-05-2024 | Cambios en puntos 5, 6 y 7, para unificar formato con anterior documento. | Alejandro Castro<br>Pablo Zalazar |

## 8.0 Documentos relacionados

- Estándar de tokens de autenticación
- Estándar de registro de seguridad
- Publicación especial del NIST 800-63-3 Pautas de identidad digital

# Capítulo 3

# Estándar de Autenticación Tokens

## 1.0 Propósito y Beneficios

El propósito de este estándar es enumerar los tokens de autenticación apropiados que se pueden usar con sistemas desarrollados u operados que requieren acceso autenticado según el Nivel de garantía del autenticador (AAL). Este documento también proporciona los requisitos para la gestión de esos dispositivos de autenticación.

## 2.0 Alcance

Esta norma se aplica a la autenticación de cuentas que acceden a sistemas de tecnología de la información con el fin de realizar actividades administrativas gubernamentales de forma electrónica.

## 3.0 Declaración de información

### 3.1 Niveles de garantía y tipos de tokens requeridos

El Nivel de Garantía del Autenticador (AAL) de un sistema determina el grado de certeza requerido al autenticar a un usuario. La siguiente tabla describe el nivel de confianza asociado con cada AAL. Estos niveles de garantía son consistentes con los establecidos por NIST[1].

| *Nivel de garantía del autenticador (AAL)* | |
|---|---|
| AAL1 | AAL1 proporciona cierta seguridad de que el usuario controla un "autenticador" vinculado a la cuenta gubernamental. AAL1 requiere autenticación de factor único (por ejemplo, contraseña) o de múltiples factores (por ejemplo, contraseña + token) utilizando los métodos de autenticación disponibles. Una autenticación exitosa requiere que la persona que inicia sesión demuestre la posesión y/o el control del autenticador, a través de un protocolo de autenticación seguro como se define en el Estándar de encriptación. |

[1]Descrito en la publicación especial del NIST 800-63-3: Pautas de identidad digital

| | |
|---|---|
| AAL2 | AAL2 proporciona una alta confianza en que el usuario controla los autenticadores vinculados a la cuenta gubernamental. Se requiere prueba de posesión y control de dos factores de autenticación distintos (multifactor) a través de protocolos de autenticación seguros. Se requieren técnicas criptográficas aprobadas, tal como se define en el Estándar de cifrado en AAL2 y superiores. |
| AAL3 | AAL3 proporciona una confianza muy alta en que el usuario controla los autenticadores vinculados a la cuenta gubernamental. La autenticación en AAL3 se basa en la prueba de posesión de una clave mediante un protocolo criptográfico. La autenticación AAL3 debe utilizar un autenticador criptográfico basado en hardware y un autenticador que proporcione resistencia a la suplantación del verificador; el mismo dispositivo puede cumplir ambos requisitos. Para autenticarse en AAL3, los usuarios deben demostrar la posesión y el control de dos factores de autenticación distintos a través de protocolos de autenticación seguros. Se requieren técnicas criptográficas aprobadas. |

La Cartera Administrativa debe identificar el nivel de aseguramiento apropiado para cada sistema. Cada nivel de seguridad requiere diferentes tokens de autenticación que incorporan uno o más factores de autenticación (es decir, algo que usted sabe, algo que tiene y algo que es). Los niveles de garantía del autenticador (AAL) 1 y 2 requieren autenticación de un solo factor. AAL 3 requiere autenticación multifactor.
Las reparticiones deben elegir los tipos de token apropiados para su nivel de seguridad de las Tablas 1 o 2. La Tabla 1 muestra el nivel de seguridad máximo que se puede lograr con un solo tipo de token.

**Tabla 1: Opciones de un solo token**

| ***Tipos de tokens*** | **AAL1** | **AAL2** | **AAL3** |
|---|---|---|---|
| ***Token secreto memorizado*** | X | | |
| ***Token de secretos de búsqueda (Look-Up Secrets)*** | X | | |
| ***Token fuera de banda*** | X | | |
| ***Dispositivo de contraseña de un solo uso*** | X | | |
| ***Dispositivo criptográfico de factor único*** | X | | |

| | | | |
|---|---|---|---|
| ***Dispositivo criptográfico de software multifactor*** | | X | |
| ***Dispositivo de hardware de contraseña única de factor múltiple*** | | X | |
| ***Dispositivo criptográfico de hardware multifactor*** | | | X |

Las reparticiones pueden usar autenticación de múltiples tokens (es decir, una combinación de tokens) para mejorar el nivel general de seguridad como se muestra en la Tabla 2. Por ejemplo, AAL3 se puede lograr usando dos tokens clasificados en AAL2 que representan dos factores de autenticación diferentes (es decir, algo que sabes, algo que tienes y algo que eres).

**Tabla 2: Opciones de múltiples tokens**

<table>
<tr><th>AL 2</th><th>AL 3</th></tr>
<tr><td>AAL 2 requiere que, una combinación de autenticadores de un solo factor incluya un autenticador secreto memorizado y un segundo factor basado en la posesión de alguna de las opciones de la siguiente lista:<ul><li>Secretos de búsqueda</li><li>Dispositivo fuera de banda</li><li>Dispositivo OTP de factor único</li><li>Software criptográfico de factor único</li><li>Dispositivo criptográfico de factor único</li></ul></td><td>AAL 3 requiere el uso de una de las siguientes combinaciones de autenticadores:<table>
<tr><td>1. Secreto memorizado</td><td><ul><li>Dispositivo criptográfico de factor único</li></ul></td></tr>
<tr><td>2. Dispositivo OTP multifactor (software y/o hardware)</td><td><ul><li>Dispositivo criptográfico de factor único</li></ul></td></tr>
<tr><td>3. Dispositivo OTP de factor único (solo hardware)</td><td><ul><li>Autenticador de software criptográfico multifactor</li></ul></td></tr>
<tr><td>4. Dispositivo OTP de factor único (solo hardware)</td><td><ul><li>Autenticador de software criptográfico de factor único</li><li>Secreto memorizado</li></ul></td></tr>
</table></td></tr>
</table>

## 3.2 Tipos de tokens de autenticación

### 3.2.1 Token secreto memorizado

Un token secreto memorizado “es algo que sabes”. Los tokens secretos memorizados suelen ser claves que combinan caracteres y números. Los ejemplos

incluyen contraseñas, frases de contraseña y números de identificación personal (PIN).
Normalmente, se utiliza un token secreto memorizado por sí solo para AAL 1. En AAL 2 y 3 **requieren** autenticación multifactor. Cuando se utiliza un token secreto memorizado como uno de los factores en una solución de autenticación multifactor, se aplican los requisitos del token en la AAL asociada.
La siguiente tabla aborda los requisitos mínimos básicos relacionados con los tokens secretos memorizados. Otros cumplimientos de seguridad, pueden necesitar requisitos mínimos más estrictos. Se deben consultar los apartados de cumplimiento relevantes para abordar sistemas, aplicaciones, etc.

**Tabla 3: Requisitos mínimos del token secreto memorizado**

<table>
<tr><th></th><th colspan="3">Niveles de garantía</th></tr>
<tr><th>Categoría</th><th>1</th><th>2[2]</th><th>3</th></tr>
<tr><td colspan="4">Estándares de gestión de contraseñas</td></tr>
<tr><td>Caducidad de la contraseña después de x días</td><td>731</td><td>183</td><td rowspan="6">Se requiere autenticación multifactor<br><br>Este tipo de token solo se puede utilizar con autenticadores seleccionados en AAL 2 y 3. Consulte la Tabla 2 para obtener más información.</td></tr>
<tr><td>Sistema para proporcionar mensajes de caducidad de contraseña que comiencen al menos x días antes de la caducidad</td><td colspan="2">14</td></tr>
<tr><td>Reutilización de contraseña</td><td colspan="2">Después de 24 contraseñas únicas</td></tr>
<tr><td>Edad mínima de la contraseña</td><td colspan="2">2 días</td></tr>
<tr><td>Número máximo de inicios de sesión de gracia después del vencimiento, para permitir el cambio de contraseña</td><td colspan="2">1</td></tr>
<tr><td>Las contraseñas temporales se cambiaron inmediatamente en el primer inicio de sesión</td><td colspan="2">Sí</td></tr>
<tr><td colspan="4">Estándares de composición de contraseñas[3]</td></tr>
<tr><td>La contraseña no debe ser la misma que el ID de usuario.</td><td colspan="2">Sí</td><td rowspan="8">Se requiere autenticación multifactor<br><br>Este tipo de token solo se puede utilizar con autenticadores seleccionados en AAL 2 y 3. Consulte la Tabla 2 para obtener más información.</td></tr>
<tr><td>Longitud mínima</td><td colspan="2">14</td></tr>
<tr><td>Número máximo de caracteres repetidos</td><td colspan="2">3</td></tr>
<tr><td>Número mínimo de letras mayúsculas</td><td colspan="2">1</td></tr>
<tr><td>Número mínimo de letras minúsculas</td><td colspan="2">1</td></tr>
<tr><td>Número mínimo de letras</td><td colspan="2">3</td></tr>
<tr><td>Número mínimo de números</td><td colspan="2">1</td></tr>
<tr><td>Número mínimo de caracteres especiales</td><td colspan="2">1</td></tr>
</table>

### 3.2.2 Look-Up Secrets

[2]Cuando se utiliza una solución multifactor para AAL2 y AAL3, según sea necesario, y uno de los factores es un secreto memorizado, se aplican los estándares AAL2.

[3]Se reconoce que no todos los sistemas podrán hacer cumplir todos estos estándares. En esos casos, se puede solicitar una solicitud de excepción al Director de Seguridad de la Información (CISO).

Es un método utilizado para recuperar un acceso perdido. Un secreto de búsqueda es algo que tienes. Es un registro físico o electrónico que almacena un conjunto de datos privados que se comparten entre el usuario y el CSP. El autenticador se utiliza para buscar los datos privados apropiados necesarios para responder a un mensaje del verificador. Un ejemplo es el uso de preguntas y respuestas privadas (secretas) permitiendo acceder a la “clave de recuperación” en caso de que el autenticador se pierda, se olvide o no funcione correctamente.
Los secretos de búsqueda se utilizan comúnmente en AAL 1. En los casos de AAL 2 y 3 requieren autenticación multifactor. Cuando se combina con un secreto memorizado, se aplican las reglas de AAL 2.
**Requisitos del autenticador:** los secretos de búsqueda deben tener al menos 4 caracteres y deben distribuirse a través de un canal seguro.

### 3.2.3 Token fuera de banda (OOB)

Los tokens OOB son algo que tienes. Son una combinación de un dispositivo físico (p. ej., teléfono celular, PDA, buscapersonas, línea fija) y un secreto que un verificador transmite al dispositivo a través de un canal de comunicaciones distinto para un uso único.
Un ejemplo de un token OOB sería un usuario que inicia sesión en un sitio web y recibe un mensaje de texto o una llamada telefónica en su teléfono celular (preregistrado con el Proveedor de servicios de credenciales (CSP) durante la fase de registro) con un autenticador aleatorio que se presentará, como parte del protocolo de autenticación. El correo electrónico no se puede utilizar para transmitir el autenticador aleatorio para el dispositivo OOB.
**Requisitos del autenticador**: el usuario debe poseer y controlar el dispositivo y debe ser direccionable de forma única. El autenticador debe establecer un canal separado con el verificador para recuperar el secreto fuera de banda o la solicitud de autenticación. El canal secundario se considera fuera de banda (incluso si termina en el mismo dispositivo) si el dispositivo no filtra información de un canal al otro sin autorización del usuario.
El uso de la Red Telefónica Pública Conmutada (PSTN) está restringido a menos que el número de teléfono registrado previamente en uso esté asociado con un dispositivo físico específico. Cambiar el número de teléfono prerregistrado equivale a vincular un nuevo autenticador y debe seguir los requisitos aplicables. No se debe utilizar el protocolo de voz sobre Internet (VOIP) ni el correo electrónico para la autenticación OOB.
**Requisitos del token**: el usuario debe poseer y controlar el token, debe ser direccionable de forma única y debe admitir la comunicación a través de un canal/protocolo independiente del canal/protocolo principal para la autenticación electrónica.
Direccionable de forma única significa que el token puede ser direccionado mediante una característica única (por ejemplo, número de teléfono).
Al acceder a una aplicación a través de un dispositivo móvil y utilizar un teléfono virtual y un sistema de gestión de comunicaciones (es decir, Google Voice), ese

dispositivo móvil no será viable como token OOB ya que no existe un canal/protocolo separado para la comunicación del autenticador aleatorio.
Una limitación con el uso de tokens OOB es que, si el dispositivo está infectado, incluso si la comunicación ocurre a través de un canal/protocolo separado, ambas formas de autenticación (acceso a la aplicación y recepción del token) se ven comprometidas y, por lo tanto, toda comunicación no es confiable.
**Requisitos del verificador**: el período de tiempo máximo que puede existir un token OOB es de 10 minutos y solo se puede usar una vez. El secreto generado por el verificador debe tener como mínimo 3 caracteres; sin embargo, cualquier secreto de autenticación que tenga menos de 8 caracteres debe limitar el número de intentos fallidos de autenticación a no más de 10.

### 3.2.4 Dispositivo criptográfico de factor único (SF)

Los dispositivos criptográficos SF son algo que tienes. Es un dispositivo de hardware que realiza operaciones criptográficas en la entrada proporcionada al dispositivo. No requiere un segundo factor. Generalmente es un mensaje firmado. Un ejemplo sería un certificado de Secure Socket Layer/Transport Layer Services (SSL/TLS).
**Requisitos del autenticador**: los módulos criptográficos utilizados deberán estar validados en FIPS 140-2, Nivel 1 o superior. También se aceptan productos validados según versiones posteriores de FIPS 140.
**Requisitos del verificador**: la entrada (por ejemplo, un nonce o desafío) para generar el token tiene al menos 8 caracteres (64 bits de entropía) y debe ser única durante la vida útil del autenticador o estadísticamente única utilizando un generador de bits aleatorios aprobado. La verificación debe utilizar criptografía aprobada.

### 3.2.5 Dispositivo de contraseña de un solo uso (OTP) de factor único (SF)

Los dispositivos SF OTP son algo que tienes. Es un dispositivo de hardware que admite la generación espontánea de OTP. Este dispositivo tiene un secreto incorporado que se utiliza como “semilla” (seed) para la generación de OTP y no requiere activación a través de un segundo factor. La autenticación se logra proporcionando una OTP aceptable y demostrando así la posesión y el control del dispositivo por parte del usuario. El dispositivo se utiliza cada vez que se requiere autenticación.
Los ejemplos incluyen tokens de llavero. Un usuario intenta iniciar sesión en un sitio web y proporciona un código generado por token u OTP.
**Requisitos del autenticador**: se debe utilizar un cifrado de bloque aprobado o una función hash para combinar una clave simétrica almacenada en el dispositivo con un nonce para generar una OTP. El nonce puede ser una fecha y hora o un contador generado en el dispositivo.
**Requisitos del verificador**: la OTP tendrá una vida útil limitada, con un máximo de 2 minutos. El módulo criptográfico que realiza las funciones de verificador deberá estar validado en FIPS 140-2 Nivel 1 o superior. También se aceptan productos validados según versiones posteriores de FIPS 140.

### 3.2.6 Token criptográfico de software multifactor (MF)

Un token criptográfico del software MF es algo que usted tiene y debe ser desbloqueado por algo que conoce o por algo que es.
Es una clave criptográfica que se almacena en un disco o en algún otro medio "soft" y debe desbloquearse mediante un segundo factor de autenticación independiente del factor de autenticación utilizado para acceder al disco u otro medio "soft".
La autenticación se logra demostrando la posesión y control de la clave. El token depende en gran medida del protocolo criptográfico específico, pero generalmente es algún tipo de mensaje firmado.
Un ejemplo sería un certificado criptográfico privado que se desbloquea mediante una frase de contraseña independiente de la que desbloquea el dispositivo en el que está almacenado el certificado. El certificado implementado en la estación de trabajo del usuario (algo que usted tiene) en combinación con una frase de contraseña (algo que conoce) proporciona autenticación multifactor. La contraseña para acceder al dispositivo no puede desbloquear automáticamente el certificado.
**Requisitos del autenticador**: el módulo criptográfico deberá estar validado en FIPS 140-2 Nivel 1 o superior. También se aceptan productos validados según versiones posteriores de FIPS 140. Cada autenticación requerirá el ingreso de la contraseña u otros datos de activación y la copia no cifrada de la clave de autenticación se borrará después de cada autenticación.
**Requisitos del verificador**: la entrada del token generado por el verificador (por ejemplo, un nonce o desafío) tiene al menos 8 caracteres (64 bits de entropía).

### 3.2.7 Dispositivo de contraseña de un solo uso (OTP) multifactor (MF)

Un dispositivo MF OTP es algo que usted tiene y debe ser desbloqueado por algo que conoce o por algo que es.
Es un dispositivo de hardware que genera OTP para usar en la autenticación y que debe desbloquearse mediante un segundo factor de autenticación. El segundo factor de autenticación se puede lograr a través de un teclado de entrada integral, un lector biométrico integral (por ejemplo, de huellas dactilares) o una interfaz directa de computadora (por ejemplo, un puerto USB).
La OTP generalmente se muestra en el dispositivo y se ingresa manualmente en el verificador como contraseña, aunque también se permite la entrada electrónica directa desde el dispositivo a una computadora.
Un ejemplo sería un token de llavero en combinación con un PIN. Un usuario intenta iniciar sesión en un sitio web y proporciona un PIN definido por el usuario (establecido cuando se asignó el token) y un código generado por el token. La combinación del PIN y el código generado por el token se denomina contraseña.
**Requisitos del autenticador**: el módulo criptográfico debe validarse en FIPS 140-2 Nivel 2 o superior y el token en sí debe cumplir con la seguridad física en FIPS 140-2 Nivel 3 o superior. Esto significa que el token es a prueba de manipulaciones; no se puede abrir para realizar ingeniería inversa u obtener un valor inicial, etc. Los productos validados según versiones posteriores de FIPS 140 también son aceptables. Consulte el Estándar de encriptación para obtener información adicional.

La OTP debe generarse utilizando un cifrado de bloque aprobado o una función hash para combinar una clave simétrica almacenada en un dispositivo de hardware personal con un nonce para generar una OTP. El nonce puede ser una fecha y hora o un contador generado en el dispositivo. Cada autenticación requerirá la introducción de una contraseña u otros datos de activación a través de un mecanismo de entrada integrado.
**Requisitos del verificador**: la OTP tendrá una vida útil limitada, con un máximo de 2 minutos.

### 3.2.8 Dispositivo criptográfico multifactor (MF)

Un dispositivo criptográfico MF es algo que usted tiene y debe ser desbloqueado por algo que conoce o por algo que es.
Es un dispositivo de hardware que contiene una clave criptográfica protegida que debe desbloquearse mediante un segundo factor de autenticación.
La autenticación se logra demostrando la posesión del dispositivo y el control de la clave. El token depende en gran medida del protocolo y dispositivo criptográfico específicos, pero generalmente es algún tipo de mensaje firmado. Por ejemplo, en Transport Layer Services (TLS), hay un mensaje de "verificación de certificado". Un ejemplo sería una tarjeta de cajero automático.
**Requisitos del autenticador**: el módulo criptográfico deberá estar validado según FIPS 140-2, nivel 2 o superior; y el token en sí cumple con la seguridad física de FIPS 140-2 Nivel 3 o superior. Esto significa que el token es a prueba de manipulaciones; no se puede abrir para realizar ingeniería inversa u obtener un valor inicial, etc. Los productos validados según versiones posteriores de FIPS 140 también son aceptables.
Se requiere el ingreso de una contraseña, PIN o datos biométricos para activar la clave de autenticación. No se permite la exportación de claves de autenticación.
**Requisitos del verificador**: la entrada del token generado por el verificador (por ejemplo, un nonce o desafío) tiene al menos 8 caracteres (64 bits de entropía).

### 3.3 Renovación/Reemisión de Tokens

Todos los tokens deben caducar dentro de los dos (2) años posteriores a su emisión. Se debe proporcionar al usuario una notificación de advertencia sobre el vencimiento del token dentro de un mínimo de 14 días antes del vencimiento.
Una vez que el token haya caducado, su uso se desactivará y/o bloqueará automáticamente.
Algunos tipos de tokens admiten el proceso de renovación, mientras que otros admiten la reemisión. Dependiendo del nivel de garantía, el usuario deberá restablecer su identidad con el CSP si el token ha caducado o demostrar la posesión del token vigente antes de que se produzca la renovación o la reemisión.

# 4.0 Cumplimiento

Los empleados que incumplan esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y/o administrativas si correspondieren. Los no empleados, incluidos, entre otros, los contratistas, pueden

estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

## 5.0 Definiciones de términos clave

| **Término** | Definición |
|---|---|
| **Token de Secreto Memorizado** | Hace referencia a “algo que sabes”, por ejemplo una contraseña. |

## 6.0 Historial de revisiones

| **Fecha** | **Descripción de Cambio** | **Crítico** |
|---|---|---|
| 06-06-2024 | Draft final del documento | Alejandro Castro<br>Pablo Zalazar |

## 7.0 Documentos relacionados

Líneas guía de identidad digital NIST 800-63
Estándar de cifrado

## 8.0 Anexo

### 8.1 Dispositivos Token Recomendados para Utilización con Sistema GDE, *Versión Provincia 4*

Dentro de la jurisdicción de la Provincia de Jujuy, el Sistema GDE ha sido desplegado en su *versión Provincia 4*. Por lo tanto, en relación con los dispositivos TOKEN, para firma digital, se recomienda lo de detallado a continuación:

Se debe adquirir un dispositivo criptográfico (token) que cumpla con el estándar FIPS 140-2 nivel 2 o superior, que soporte claves RSA de 2048 bits. Los mismos deberán alinearse a lo recomendado en los estándares NIST (National Institute of Standards and Technology).

Además, deberá tratarse los dispositivos criptográficos del fabricante cuya marca, modelo, versión de hardware y firmware coincida con lo declarado en la correspondiente

Certificación FIPS 140, limitando el no uso de dispositivos criptográficos del tipo OEM (Original Equipment Manufacturer).

## Modelos Testeados tipo:

- **mToken CryptoID:** mToken CryptoID soporta aplicaciones basadas en los estándares de la industria CAPI y PKCS#11, como Windows smartcard logon, VPN (Cisco, Checkpoint, OpenVPN), Bit Locker, Internet Explorer, Mozilla Firefox, Google Chrome, etc.
- **EnterSafe ePass2003 X15:** ePass2003 utiliza los estándares de la industria como son el Microsoft MiniDriver, Microsoft Crypto API y el estándar PKCS#11. Adicionalmente soporta múltiples tipos de certificados y pares de llaves. Todas las aplicaciones compatibles con estos estándares pueden ser integradas con ePass2003.
- **SafeNet Etoken 5110:** Los SafeNet eToken 5110 (nueva versión del eToken PRO / 5100) son dispositivos criptográficos USB portables para la autenticación de usuarios basados en la misma tecnología de las tarjetas inteligentes. Esta tecnología de certificados (PKI), le permite generar y almacenar credenciales tales como claves privadas, contraseñas y certificados digitales, dentro del ambiente protegido del chip del token.

# Capítulo 4

# Políticas de identificación y autenticación

## 1.0 OBJETIVO

Garantizar que solo los usuarios y dispositivos debidamente identificados y autenticados tengan acceso a los recursos de tecnología de la información (TI) de conformidad con las políticas, estándares y procedimientos de seguridad de TI.

## 2.0 POLÍTICA

Esta política es aplicable a todos los departamentos y usuarios de recursos y activos de TI.

2.1 IDENTIFICACIÓN Y AUTENTICACIÓN

El Departamento de TI deberá:

a. Garantizar que los sistemas de información identifiquen y autentiquen de forma única a los usuarios o procesos que actúan en nombre de los usuarios del Gobierno de Jujuy.

b. Asegurarse de que los sistemas de información implementen autenticación multifactor para el acceso a la red de cuentas privilegiadas.

c. Asegurarse de que los sistemas de información implementen autenticación multifactor para el acceso a la red de cuentas sin privilegios.

d. Garantizar que los sistemas de información implementen autenticación multifactor para el acceso local de cuentas privilegiadas.

e. Asegurarse de que los sistemas de información implementen mecanismos de autenticación resistentes a la repetición para el acceso a la red de cuentas privilegiadas.

f. Asegurarse de que los sistemas de información implementen autenticación multifactor para el acceso remoto a cuentas privilegiadas y no privilegiadas, de modo que uno de los factores sea proporcionado por un dispositivo separado del sistema que obtiene acceso y el dispositivo utilice mecanismos criptográficos de seguridad que protejan el token de autenticación principal (clave secreta, clave privada o contraseña de un solo uso) contra el compromiso por amenazas de protocolo que incluyen: escuchas ilegales, repetición, adivinanzas en línea, suplantación de verificador y ataques de man-in-the-middle.

g. Asegúrese de que los sistemas de información acepten y verifiquen electrónicamente las credenciales de Verificación de Identidad Personal (PIV).

2.2 IDENTIFICACIÓN Y AUTENTICACIÓN DEL DISPOSITIVO

El Departamento de TI deberá:

a. Asegurarse de que los sistemas de información identifiquen y autentiquen de forma única todos los dispositivos antes de establecer una conexión de red.

2.3 GESTIÓN DE IDENTIFICADORES

El Departamento de TI, a través de los administradores o encargados de los sistemas de información del departamento, deberá:

a. Asegurarse de que el Gobierno de Jujuy administre los identificadores del sistema de información recibiendo autorización del CISO o encargado de Seguridad Informática para asignar un identificador de individuo, grupo, rol o dispositivo.

b. Seleccionar un identificador único que identifique a un individuo, grupo, función o dispositivo.

c. Asignar el identificador al individuo, grupo, función o dispositivo previsto.

d. Evitar la reutilización de identificadores durante 90 días, salvo que exista alguna política gubernamental más restrictiva que la mencionada.

e. Desactivar el identificador después de 30 días de inactividad.

2.4 GESTIÓN DE AUTENTICADORES

El Departamento de TI deberá:

a. Administrar los autenticadores del sistema de información verificando, como parte de la distribución inicial del autenticador, la identidad del individuo, grupo, rol o dispositivo que recibe el autenticador.

b. Establecer contenido de autenticador inicial para los autenticadores definidos por la organización.

c. Asegurarse de que los autenticadores tengan un mecanismo suficientemente resistente para el uso previsto.

d. Establecer e implementar procedimientos administrativos para la distribución inicial de autenticadores, para autenticadores perdidos, comprometidos o dañados, y para revocar autenticadores.

e. Cambiar el contenido predeterminado de los autenticadores antes de la instalación del sistema de información.

f. Establecer restricciones de vida mínimas y máximas y condiciones de reutilización para los autenticadores.

g. Implementar mecanismos que permitan cambiar/actualizar los autenticadores cada 90 días.

h. Proteger el contenido del autenticador contra divulgación y modificación no autorizadas.

i. Requerir que las personas y los dispositivos implementen las medidas de seguridad específicas para proteger a los autenticadores.

j. Cambiar los autenticadores para cuentas de grupo/rol cuando cambie la membresía en esas cuentas.

k. Asegurarse de que los sistemas de información, para la autenticación basada en contraseñas, apliquen una complejidad mínima de contraseña que no debe contener el valor completo del Nombre de cuenta o el valor completo del Nombre del usuario.

l. Asegúrese de que las contraseñas contengan caracteres de **cuatro** de las siguientes cinco categorías, siendo las primeras 4 obligatorias:

    i. Caracteres en mayúsculas de idiomas español (de la A a la Z)

    ii. Caracteres en minúscula de idiomas español (de la a a la z);

    iii. Base 10 dígitos (0 a 9);

    iv. Caracteres no alfanuméricos ~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/ ; y

    v. Cualquier carácter Unicode que esté categorizado como carácter alfabético, pero que no esté en mayúsculas ni en minúsculas.

m. Requerir que las contraseñas tengan una longitud mínima de 14 caracteres.

n. Aplicar al menos un carácter cambiado cuando se crean nuevas contraseñas.

o. Almacenar y transmitir únicamente contraseñas protegidas criptográficamente.

p. Aplicar restricciones de vida mínima y máxima de contraseña de un día y 120 días respectivamente.

q. Prohibir la reutilización de contraseñas durante 12 (doce) generaciones.

r. Permitir el uso de una contraseña temporal para iniciar sesión en el sistema con un cambio inmediato a una contraseña permanente.

s. Asegúrese de que el sistema de información, para la autenticación basada en PKI, valide las certificaciones mediante la construcción y verificación de una ruta de certificación hacia una entidad certificadora de confianza aceptada, incluida la verificación de la información del estado del certificado.

t. Hacer cumplir el acceso autorizado a la clave privada correspondiente.

u. Asignar la identidad autenticada a la cuenta del individuo o grupo.

v. Implementar un caché local de datos de revocación para respaldar el descubrimiento y la validación de rutas en caso de que no se pueda acceder a la información de revocación a través de la red.

w. Requerir que el proceso de registro para recibir los accesos/credenciales específicos se lleve a cabo en persona o por un tercero confiable ante las Autoridades del Departamento de TI con autorización de CISO o Encargado de Seguridad.

x. Garantizar que el sistema de información, para la autenticación basada en tokens de hardware, emplee mecanismos que satisfagan los requisitos de calidad de tokens definidos por el Gobierno de Jujuy.

2.5 COMENTARIOS DEL AUTENTICADOR

El Departamento de TI deberá:

a. Asegurarse de que los sistemas de información oculten la retroalimentación de la información de autenticación durante el proceso de autenticación para proteger la información de una posible explotación/uso por parte de personas no autorizadas.

2.6 AUTENTICACIÓN DEL MÓDULO CRIPTOGRÁFICO

El Departamento de TI deberá:

a. Asegurar que los sistemas de información implementen mecanismos de autenticación a un módulo criptográfico que cumplan con los requisitos de las leyes, directivas, políticas, regulaciones, estándares y guías estatales y federales aplicables para dicha autenticación.

2.7 IDENTIFICACIÓN Y AUTENTICACIÓN

El Departamento de TI deberá:

a. Garantizar que los sistemas de información identifiquen y autentiquen de forma única a usuarios, o procesos que actúen en nombre de usuarios, en ambos casos que no sean entidades.

b. Asegurarse de que los sistemas de información acepten y verifiquen electrónicamente las credenciales de Verificación de Identidad Personal (PIV) de otras agencias gubernamentales.

c. Asegurarse de que los sistemas de información acepten únicamente credenciales de terceros aprobadas por la iniciativa el Gobierno Provincial y Nacional.

d. Asegurarse de que la organización emplee únicamente componentes de sistemas de información aprobados por el Gobierno Provincial y Nacional en sistemas de información definidos por el Gobierno de Jujuy para aceptar credenciales de terceros.

## 3.0 CUMPLIMIENTO

Los empleados que incumplan esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y/o administrativas si correspondieren. Los no empleados, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

## 4.0 EXCEPCIONES DE POLÍTICA

Las solicitudes de excepciones a esta política serán revisadas por el Director de Ciberseguridad (DC) y la Secretaría de Innovación Pública (SIP) y/o Encargado de Seguridad de la Información. Los departamentos que soliciten excepciones deberán proporcionar dichas solicitudes al DC/SIP. La solicitud debe indicar específicamente el alcance de la excepción junto con la justificación para otorgar la excepción, el posible impacto o riesgo asociado al otorgar la excepción, las medidas de mitigación de riesgos que debe tomar el Departamento de TI, iniciativas, acciones y un cronograma para lograrlo, el nivel mínimo de cumplimiento de las políticas aquí establecidas. El DC/SIP revisará dichas solicitudes; consultar con el departamento solicitante.

## 5.0 DEPARTAMENTO RESPONSABLE

Oficina principal de información y propietarios de sistemas de información de la Provincia de Jujuy.

## 6.0 HISTORIAL DE REVISIONES

| Fecha | Descripción de Cambio | Crítico |
|---|---|---|

| | | |
|---|---|---|
| 27-05-2024 | Draft final del documento | Alejandro Castro<br>Pablo Zalazar |

# Capítulo 5

# Estándar de TI: Estándar de Acceso Remoto

## 1.0 Propósito y Beneficios

El propósito de este estándar es establecer métodos autorizados para acceder de forma remota a recursos y servicios de forma segura.

Los principales problemas de seguridad con el acceso remoto incluyen la falta de controles de seguridad físicos, el uso de redes no seguras, la conexión de dispositivos infectados a redes internas, la disponibilidad de recursos internos para hosts externos, posibles daños a los recursos y el acceso no autorizado a la información.

## 2.0 Alcance

Esta norma se aplica a la autenticación de cuentas que acceden a sistemas de tecnología de la información con el fin de realizar actividades administrativas gubernamentales de forma electrónica remota.

## 3.0 Declaración de información

Se permite el acceso remoto cuando existe una necesidad administrativa clara y documentada. Se puede permitir el acceso desde dispositivos emitidos por la entidad o de propiedad personal, a discreción del MPEyM y de acuerdo con los estándares a continuación. Dicho acceso debe limitarse únicamente a aquellos sistemas necesarios para las funciones necesarias.

### 3.1 Métodos aprobados de acceso remoto

Los métodos aprobados de acceso remoto a los sistemas se enumeran en orden de preferencia.

a. **Portales**- un servidor que ofrece acceso a una o más aplicaciones a través de una única interfaz centralizada que proporciona autenticación (por ejemplo, portal basado en web, interfaz de escritorio virtual (VDI)).

b. **Acceso directo a la aplicación**– acceder a un sistema directamente con los métodos de seguridad proporcionados por la misma aplicación (por ejemplo, correo web, https).

c. **Control remoto del sistema**– controlar un sistema a distancia desde una ubicación distinta de la red **interna** del Gobierno de Jujuy.

d. **Túnel**- un canal de comunicación seguro a través del cual se puede transmitir información entre redes (por ejemplo, Red Privada Virtual (VPN)).

### 3.2 Controles requeridos

a. Cualquier método de acceso remoto debe utilizar un sistema de autenticación administrado centralmente para la administración y el acceso de los usuarios.

b. Los dispositivos y el software utilizados para el acceso remoto deben ser aprobados después de la revisión por parte del Oficial de Seguridad de la Información/responsable de seguridad designado. Se pueden proporcionar aprobaciones generales basadas en esta revisión.

c. El token de autenticación utilizado para el acceso remoto debe cumplir con los requisitos del nivel de garantía adecuado.

d. Las sesiones de acceso remoto deben requerir una nueva autenticación después de 30 minutos de inactividad.

e. Las sesiones de acceso remoto no deben durar más de 08 horas.

f. La entidad debe monitorear conexiones remotas no autorizadas y otras actividades anómalas y tomar las medidas apropiadas de respuesta a incidentes según lo establecido en Estándar de respuesta a incidentes cibernéticos.

g. Controles específicos de túneles:

    (a) Se permiten túneles divididos. (Split Tunneling)

    (b) Se requieren controles de red que regulen el acceso remoto del *endpoint*; entre dispositivos remotos y las redes involucradas.

    (c) Cuando un dispositivo de acceso remoto tenga acceso a otros dispositivos conectados en red en la red interna laboral, el dispositivo remoto debe autenticarse de manera que la configuración del dispositivo cumpla con las políticas aplicables.

## 4.0 Cumplimiento

Los empleados que incumplan esta política pueden estar sujetos a medidas disciplinarias apropiadas, así como sanciones penales, civiles y/o administrativas si correspondieren. Los no empleados, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

## 5.0 Definiciones de términos clave

| Término | Definición |
|---|---|

| | |
|---|---|
| Endpoint | Es un dispositivo cualquiera que se encuentre conectado a una red informática. |
| Split Tunneling | Un túnel dividido en una VPN, permite enrutar parte del tráfico (por ejemplo, de las aplicaciones laborales) mientras que el tráfico a internet se enruta por el acceso a internet local de la red. |

## 6.0 Historial de revisiones

| Fecha | Descripción de Cambio | Crítico |
|---|---|---|
| 13-06-2024 | Draft final del documento | Alejandro Castro<br>Pablo Zalazar |
| 14-06-2024 | Agregados en 6.0 Términos Clave, arreglos menores en documento. | Alejandro Castro |

## 7.0 Documentos relacionados

Publicación especial 800-46 del Instituto Nacional de Estándares y Tecnología (NIST), Guía para el teletrabajo empresarial y la seguridad del acceso remoto

Publicación especial del NIST 800-113, Guía de VPN SSL

Publicación especial del NIST 800-114, Guía del usuario para proteger dispositivos externos para teletrabajo y acceso remoto

# Capítulo 6

# Políticas de Seguridad Personal

### 1.0 OBJETIVO

Garantizar que las políticas de seguridad del personal sean aplicadas al acceso y uso de los recursos y datos de tecnología de la información.

### 2.0 REFERENCIA

Publicaciones especiales (SP) del Instituto Nacional de Estándares y Tecnología (NIST): NIST SP 800-53a – Seguridad del personal (PS), NIST SP 800-12, NIST SP 800-60, NIST SP 800-73, NIST SP 800-78, NIST SP 800-100; Código Electrónico de Regulaciones Federales (CFR): 5 CFR731.106; Estándares federales de procesamiento de información (FIPS)199 y 201; Directiva de la Comunidad de Inteligencia (ICD)704 Normas de seguridad del personal.

### 3.0 POLÍTICA

Esta política es aplicable a todos los departamentos y usuarios de recursos y activos de TI.

1. DESIGNACIÓN DE RIESGO DE CARGOS
   La tecnología de la información (TI) deberá:

   a. Designación de riesgo a todos los cargos.

   b. Establecer criterios de selección para las personas que ocupan esos cargos.

   c. Revisar y actualizar las designaciones de riesgo de cargos anualmente.

2. SELECCIÓN DE PERSONAL
   Los propietarios de aplicaciones y sistemas de departamentos y TI deberán:

   a. Validar la identidad de las personas antes de autorizar el acceso a los sistemas de información.

   b. Re-validar identidad de los individuos cada dos años, pudiendo disponerse revalidas extraordinarias en caso necesario

   c. Asegúrese de que las actividades de selección y revalidación del personal reflejen las leyes, directivas, regulaciones, políticas, estándares, orientación y criterios específicos estatales y federales aplicables establecidos para las designaciones de riesgo de los puestos asignados.

3. CESE DE FUNCIONES DEL PERSONAL
   Los departamentos deberán, al terminar las funciones por cualquier causa jurídica, traslado, jubilación, cese de contrato, cesantía o exoneración:

   a. Deshabilitar inmediatamente el acceso al sistema de información.

   b. Terminar/revocar cualquier autenticador/credencial asociado con el individuo.

   c. Realizar entrevistas de salida que incluyan una conversación sobre temas de seguridad de la información definidos por la repartición.

   d. Recuperar toda la propiedad relacionada con el sistema de información relacionada con la seguridad.

   e. Conservar el acceso a la información y a los sistemas de información anteriormente controlados por la persona desvinculada, por cuestiones de Auditoria, o demás tareas que se requieran.

   f. Notificar a la Unidad de Organización a la que pertenecía la persona desvinculada, la obligación de adoptar las medidas referidas precedentemente.

      La propiedad relacionada con el sistema de información incluye, por ejemplo, tokens de autenticación de hardware, manuales técnicos de administración del sistema, llaves, tarjetas de identificación y pases de construcción. Las entrevistas de salida garantizan que las personas desvinculadas comprendan las limitaciones de seguridad impuestas por ser exempleados y que se logre la responsabilidad adecuada por la propiedad relacionada con el sistema de información. Los temas de seguridad de interés en las entrevistas de salida pueden incluir, por ejemplo, recordar a las personas desvinculadas sobre los acuerdos de confidencialidad y las posibles limitaciones en el empleo futuro. Es posible que algunas personas desvinculadas no puedan realizar entrevistas de salida.

   La Repartición deberá:

   g. Notificar a las personas desvinculadas sobre los requisitos post-empleo aplicables y legalmente vinculantes para la protección de la información.

   h. Exigir que las personas desvinculadas despedidas firmen un reconocimiento de los requisitos posteriores al empleo como parte del proceso de desvinculación según lo indique el Abogado y Recursos Humanos (RR.HH.).

   i. Emplear mecanismos automatizados para notificar el cese de servicios de una persona humana.

4. TRASLADO DEL PERSONAL

Los departamentos deberán:

a) Revisar y confirmar la necesidad operativa continua de autorizaciones de acceso físico y lógico actuales a sistemas/instalaciones de información cuando las personas sean reasignadas o transferidas a otras posiciones.

b) Iniciar inmediatamente después de la transferencia formal, acciones de reasignación definidas por la repartición.

c) Modificar la autorización de acceso según sea necesario para corresponder con cualquier cambio en la necesidad operativa debido a una reasignación o transferencia.

d) Notificar a la Unidad de Organización a la que pertenecía la persona transferida, la obligación de adoptar las medidas referidas precedentemente.

Este control se aplica cuando las reasignaciones o traslados de personas son permanentes o de duración tan prolongada que justifican las acciones.

5. PROCEDIMIENTOS DE ACCESO
Los departamentos deberán:

a. Desarrollar y documentar procedimiento de acceso a sistemas de información.

b. Revisar y actualizar semestralmente los procedimientos de acceso.

c. Garantizar que las personas que requieran acceso a la información y a los sistemas de información:

i. Firmen los acuerdos de acceso adecuados antes de que se le conceda el acceso.

ii. Vuelvan a firmar las actas de procedimientos de acceso para mantener el acceso a los sistemas de información cuando los mismos hayan sido actualizados. En el caso de personal contratado debe firmarse anualmente. En caso de personal permanente o funcionarios, cuando se produzca un cambio de funciones.

Las actas acuerdos de acceso incluyen, por ejemplo, acuerdos de confidencialidad, acuerdos de uso aceptable, reglas de conducta y acuerdos de conflicto de intereses.

6. SEGURIDAD DEL PERSONAL DE TERCEROS
El Departamento de TI deberá:

a. Establecer y documentar los requisitos de seguridad del personal, incluidas las funciones y responsabilidades de seguridad de los proveedores/consultores externos.

b. Exigir a los proveedores/consultores el cumplimiento de las políticas y procedimientos de seguridad del personal establecidos por la entidad.

c. Requerir que los proveedores/consultores externos notifiquen a de cualquier transferencia de personal o despidos de personal de terceros que posean credenciales y/o insignias, o que tengan privilegios de sistemas de información dentro de las 24 horas.

d. Supervisar el cumplimiento del proveedor.
Los proveedores externos incluyen, por ejemplo, oficinas de servicios, contratistas y otras organizaciones que brindan desarrollo de sistemas de información, servicios de tecnología de la información, aplicaciones subcontratadas y gestión de redes y seguridad.

7. SANCIONES PERSONALES
TI y RRHH deberán:

a. Emplear un proceso de sanción formal de acuerdo con el Estatuto para el Personal de la Administración Pública de la Provincia de Jujuy, Ley 3161 y sus modificatorias, para las personas que no cumplan con las políticas y procedimientos de seguridad de la información establecidos.

b. Notificar dentro de las 24 horas cuando se inicia un proceso formal de sanciones a los empleados, en los términos actuales del artículo 173 incisos 4° a 8° del Estatuto para el Personal de la Administración Pública de la Provincia de Jujuy, Ley 3161.

## 4.0 CUMPLIMIENTO

Los empleados que violen esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y/o administrativas si correspondieren. Los terceros/proveedores, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

## 5.0 EXCEPCIONES DE POLÍTICA

Las solicitudes de excepciones a esta política serán revisadas por el Director de Ciberseguridad de la Información (DC), la Secretaría de Innovación Pública (SIP) y/o Encargado de Seguridad de la Información. Los departamentos que soliciten excepciones

deberán proporcionar dichas solicitudes al DC/SIP. La solicitud debe indicar específicamente el alcance de la excepción junto con la justificación para otorgar la excepción, el posible impacto o riesgo asociado al otorgar la excepción, las medidas de mitigación de riesgos que debe tomar el Departamento de TI, iniciativas, acciones y un cronograma para lograrlo, el nivel mínimo de cumplimiento de las políticas aquí establecidas. El DC/SIP revisará dichas solicitudes; consultar con el departamento solicitante.

## 6.0 HISTORIAL DE REVISIONES

| Fecha | Descripción de Cambio | Crítico |
|---|---|---|
| 25-06-2024 | Draft final del documento | Alejandro Castro<br>Pablo Zalazar |

# Capítulo 7

# Políticas de concientización y entrenamiento en seguridad

### 1.0 OBJETIVO

Garantizar que se brinde el nivel adecuado de capacitación en concientización sobre seguridad de la información a todos los usuarios de Tecnología de la Información (TI).

### 2.0 REFERENCIAS

Publicaciones especiales del Instituto Nacional de Estándares y Tecnología (NIST): NIST SP 800-53: Concientización y capacitación (AT), NIST SP 800-12, NIST SP 800-16, NIST SP 800-50, NIST SP 800-100; Código Electrónico de Regulaciones Federales (CFR): 5 CFR 930.301

### 3.0 POLÍTICA

Esta política es aplicable a todos los departamentos y usuarios de recursos y activos de TI.

1. FORMACIÓN DE CONCIENTIZACIÓN EN SEGURIDAD
   *El Ministerio de Planificación Estratégica y Modernización* - MPEyM deberá:

   a. Programar capacitación en concientización sobre seguridad como parte de la capacitación inicial para nuevos usuarios.

   b. Programar capacitación en concientización sobre seguridad cuando lo requieran los cambios en el sistema de información y periódicamente con la frecuencia necesaria en cada Unidad de Organización.

   c. La oficina de TI determinará el contenido adecuado de la formación en materia de concienciación sobre la seguridad y las técnicas de concienciación sobre la seguridad en función de los requisitos organizativos específicos y los sistemas de información a los que el personal tiene acceso autorizado. El contenido deberá:

      i. Incluir una comprensión básica de la necesidad de seguridad de la información y acciones de los usuarios para mantener la seguridad y responder a incidentes de seguridad sospechosos.

      ii. Abordar la concientización sobre la necesidad de seguridad en las operaciones. Las técnicas de concientización sobre la seguridad pueden incluir, por ejemplo, exhibir carteles, ofrecer suministros con recordatorios

de seguridad, generar avisos por correo electrónico de altos funcionarios de la organización, mostrar mensajes en la pantalla de inicio de sesión y realizar eventos de concientización sobre la seguridad de la información.

2. CONCIENCIA EN SEGURIDAD | AMENAZA INTERNA
   El Departamento de TI deberá:

   a. Incluir capacitación en concientización sobre seguridad para reconocer e informar indicadores potenciales de amenazas internas.

3. FORMACIÓN EN SEGURIDAD BASADA EN FUNCIONES
   El Departamento de TI deberá:

   a. Proporcionar capacitación en seguridad basada en roles al personal con roles y responsabilidades de seguridad asignados:

      i. Antes de autorizar el acceso al sistema de información o realizar las funciones asignadas.

      ii. Cuando lo requieran cambios en el sistema de información y una frecuencia periódica definida por MPEyM, después de eso.

   b. Designar personal para recibir capacitación inicial y continua en el empleo y operación de controles ambientales que incluyan, por ejemplo, dispositivos/sistemas de detección y extinción de incendios, sistemas de rociadores, extintores de incendios portátiles, mangueras fijas contra incendios, detectores de humo, temperatura/humedad, HVAC, y energía dentro de la instalación.

4. CONTROLES DE SEGURIDAD FÍSICA
   El Departamento de TI deberá:

   a. Proporcionar capacitación inicial y continua en el empleo y operación de controles de seguridad física; Los controles de seguridad física incluyen, por ejemplo, dispositivos de control de acceso físico, alarmas de intrusión física, equipos de monitoreo/vigilancia y guardias de seguridad (procedimientos operativos y de implementación).

   b. Identificar personal con roles y responsabilidades específicas asociadas con los controles de seguridad física que requieren capacitación especializada.

5. EJERCICIOS PRACTICOS
   La oficina de TI deberá:

   a. Proporcionar ejercicios prácticos de formación en seguridad que refuercen los objetivos de la formación; Los ejercicios prácticos pueden incluir, por ejemplo,

capacitación en seguridad para desarrolladores de software que incluya ataques cibernéticos simulados que exploten vulnerabilidades comunes del software (por ejemplo, desbordamientos de buffer), o ataques de phishing dirigidos a líderes/ejecutivos de alto nivel. Este tipo de ejercicios prácticos ayudan a los desarrolladores a comprender mejor los efectos de dichas vulnerabilidades y a apreciar la necesidad de estándares y procesos de codificación segura.

6. COMUNICACIONES SOSPECHOSAS Y COMPORTAMIENTO ANÓMALO DEL SISTEMA
   La oficina de TI deberá:

   a. Proporcionar capacitación a su personal específico sobre cómo reconocer comunicaciones sospechosas y comportamientos anómalos en los sistemas de información organizacionales.

7. REGISTROS DE ENTRENAMIENTO EN SEGURIDAD
   El MPEyM deberá:

   a. Designar personal para documentar y monitorear las actividades individuales de capacitación en seguridad de sistemas de información, incluida la capacitación básica en concientización sobre seguridad y la capacitación específica en seguridad de sistemas de información.

   b. Conservar registros de capacitación individuales por una periodicidad de cinco años.

## 4.0 CUMPLIMIENTO

Los empleados que incumplan esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y/o administrativas si correspondieren. Los terceros/proveedores, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

## 5.0 EXCEPCIONES DE POLÍTICA

Las solicitudes de excepciones a esta política serán revisadas por la Dirección de Ciberseguridad (DC), la Secretaría de Innovación Pública (SIP) y/o Encargado de Seguridad de la Información. Los departamentos que soliciten excepciones deberán proporcionar dichas solicitudes al DC/SIP. La solicitud debe indicar específicamente el alcance de la excepción junto con la justificación para otorgar la excepción, el posible impacto o riesgo asociado al otorgar la excepción, las medidas de mitigación de riesgos que debe tomar el Departamento de TI, iniciativas, acciones y un cronograma para lograrlo, el nivel mínimo de cumplimiento de las políticas aquí establecidas. El DC/SIP revisará dichas solicitudes; consultar con el departamento solicitante.

## 6.0 FECHA DE EMISIÓN/FECHA DE REVISIÓN

| Fecha | Descripción de Cambio | Crítico |
|---|---|---|
| 26-06-2024 | Draft final del documento | Alejandro Castro<br>Pablo Zalazar |

# Capítulo 8

# Estándar de TI: Política de uso aceptable de recursos de tecnología de la información

## 1.0 Propósito y Beneficios

El uso adecuado por parte de la Repartición respecto de la información y de los recursos de TI, así como la seguridad eficaz de dichos recursos, requieren la participación y el apoyo del personal de la Repartición ("usuarios"). Un uso inadecuado expone a la Repartición a riesgos potenciales como ataques de virus, compromiso de los sistemas, servicios de red y problemas legales.

## 2.0 Alcance

Esta política se aplica a los usuarios de cualquier sistema de información o infraestructura física, independientemente de su forma o formato, creado o utilizado para soportar la organización. Es responsabilidad del usuario leer y comprender esta política y realizar sus actividades de acuerdo con sus términos. Además, los usuarios deben leer y comprender la Política de seguridad de la información del Gobierno de la Provincia de Jujuy y sus estándares asociados.

3.0 Declaración de información

Excepto por cualquier privilegio o confidencialidad reconocido por la ley, las personas no tienen expectativas legítimas de privacidad durante el uso de los recursos de TI de la organización o de cualquier dato sobre esos recursos. Cualquier uso puede ser monitoreado, interceptado, grabado, leído, copiado, accedido o capturado de cualquier manera, incluso en tiempo real, y utilizado o divulgado de cualquier manera, por personal autorizado sin previo aviso adicional a las personas. Se realizará un monitoreo periódico de los sistemas utilizados, incluidos, entre otros: todos los archivos informáticos; y todas las formas de comunicación electrónica (incluidos correo electrónico, mensajes de texto, mensajería instantánea, teléfonos, sistemas informáticos y otros registros electrónicos). Además del aviso proporcionado en esta política, los usuarios también pueden ser notificados con un mensaje de texto de advertencia en los puntos de entrada del sistema donde los usuarios inician sesión para ser monitoreados y se les puede recordar que no se permite el uso no autorizado de los recursos de TI de la Repartición.

El MPEyM puede imponer restricciones, sobre el uso de un recurso de TI en particular. Por ejemplo, el MPEyM puede bloquear el acceso a ciertos sitios web o servicios que no sirven para fines comerciales legítimos o puede restringir la capacidad del usuario para conectar dispositivos a los recursos de TI de la organización (por ejemplo, unidades USB personales, iPods, etc).

Los usuarios que accedan a las aplicaciones y recursos TI de la organización a través de dispositivos personales, sólo deberán hacerlo con la aprobación o autorización previa de la Repartición.

**Uso Aceptable**

Todos los usos de la información y los recursos de tecnología de la información deben cumplir con las políticas, estándares, procedimientos y directrices de la organización, así como con los acuerdos de licencia y las leyes aplicables, incluidas las leyes nacionales, provinciales y de propiedad intelectual.
Consistente con lo anterior, el uso aceptable de la información y los recursos informáticos comprende los siguientes deberes:

- Comprender los controles básicos de seguridad de la información necesarios para proteger la confidencialidad, integridad y disponibilidad de la información;
- Proteger la información y los recursos de la organización del uso o divulgación no autorizados;
- Proteger información personal, privado, sensible o confidencial procedente de uso o divulgación no autorizados;
- Observar los niveles autorizados de acceso y utilizar únicamente dispositivos o servicios de tecnología de TI aprobados; y
- Informar de inmediato sospechas de incidentes o brechas de seguridad de la información a la autoridad correspondiente, ya sea la Dirección de Ciberseguridad (DC), la Secretaría de Innovación Pública (SIP) o encargado de seguridad designado.

### 3.1 Uso inaceptable

La siguiente lista no pretende ser exhaustiva, pero es un intento de proporcionar un marco para las actividades que constituyen un uso inaceptable. Sin embargo, los usuarios pueden estar exentos de una o más de estas restricciones durante sus responsabilidades laborales autorizadas, después de la aprobación de la autoridad correspondiente de la Repartición, en consulta con el personal de TI de la organización (por ejemplo, almacenamiento de material objetable en el contexto de un asunto disciplinario).
El uso inaceptable incluye, entre otros, lo siguiente:

- Uso o divulgación no autorizados de información personal, privada, sensible y/o confidencial;
- Uso o divulgación no autorizados de información y recursos de la Repartición;
- Distribuir, transmitir, publicar o almacenar cualquier comunicación, material o correspondencia electrónica que sea amenazante, obscena, acosadora, pornográfica, ofensiva, difamatoria, discriminatoria, provocativa, ilegal o intencionalmente falsa o inexacta;
- Intentar representar a la Repartición en asuntos no relacionados con los deberes o responsabilidades laborales autorizados oficialmente;
- Conectar dispositivos no aprobados a la red de la Repartición o cualquier recurso de TI;

- Conectar recursos de TI de la Repartición a redes no autorizadas;
- Conectarse a cualquier red inalámbrica mientras está físicamente conectado a la red cableada de la Repartición;
- Instalar, descargar o ejecutar software que no haya sido aprobado después de una revisión adecuada de seguridad, legal y/o de TI de acuerdo con las políticas de la Repartición;
- Conectarse a sistemas de correo electrónico externos (por ejemplo, Gmail, Hotmail, Yahoo) sin la aprobación previa de la Repartición (El gobierno de la Provincia debe reconocer el riesgo inherente al uso de servicios de correo electrónico externos, ya que el correo electrónico se utiliza a menudo para distribuir malware);
- Usar los recursos de TI de una organización para hacer circular solicitudes o anuncios no autorizados para fines no gubernamentales, incluidas entidades religiosas, políticas o sin fines de lucro;
- Proporcionar a terceros no autorizados, incluidos familiares y amigos, acceso a la información, los recursos o las instalaciones de TI de la organización;
- Usar información o recursos de TI de la Repartición para fines comerciales o personales, en apoyo de actividades "con fines de lucro" o en apoyo de otro empleo o actividad comercial externa (por ejemplo, consultoría remunerada, transacciones comerciales, etc);
- Propagar comunicaciones en cadena, correos masivos fraudulentos, spam u otros tipos de contenido de correo electrónico no deseado, utilizando recursos de TI de la organización; y
- Manipular, desconectar o eludir de otro modo los controles de seguridad de TI de la Repartición o de terceros.

### 3.2 Uso Personal Ocasional e Incidental

Se permite el uso personal ocasional, incidental y necesario de los recursos de TI, siempre que dicho uso: sea consistente con esta política; está limitado en cantidad y duración; y no impide la capacidad del individuo u otros usuarios para cumplir con las responsabilidades y deberes del Gobierno, incluidos, entre otros, el uso extensivo de ancho de banda, recursos o almacenamiento. Es importante ejercer buen juicio con respecto al uso personal ocasional e incidental. Las Reparticiones pueden revocar o limitar este privilegio en cualquier momento.

### 3.3 Responsabilidad Individual

Se requiere responsabilidad individual al acceder a todos los recursos de TI y la información de la Repartición. Todos son responsables de protegerse contra actividades no autorizadas realizadas con su ID de usuario. Esto incluye bloquear la pantalla de su computadora cuando se aleja de su sistema y proteger sus credenciales

(por ejemplo, contraseñas, tokens o tecnología similar) contra divulgación no autorizada. Las credenciales deben tratarse como información confidencial y no deben divulgarse ni compartirse bajo ninguna circunstancia.

### 3.4 Restricciones a la transmisión y almacenamiento de información fuera del sitio

Los usuarios no deben transmitir información restringida de la organización, no pública, personal, privada, sensible o confidencial hacia o desde cuentas de correo electrónico personales (por ejemplo, Gmail, Hotmail, Yahoo) ni utilizar una cuenta de correo electrónico personal para realizar las labores de la Repartición a menos que estén autorizados explícitamente. Los usuarios no deben almacenar información restringida del Gobierno, no pública, personal, privada, sensible o confidencial en un dispositivo emitido por otra Entidad o con un servicio de almacenamiento de archivos de terceros que no haya sido aprobado para dicho almacenamiento por la Provincia de Jujuy.
Los dispositivos que contienen información gubernamental deben estar atendidos en todo momento o asegurados físicamente y no deben ser registrados en los sistemas de equipaje de los transportistas.

### 3.5 Responsabilidad del usuario por los equipos de TI

A los usuarios se les asigna o se les da acceso rutinariamente a equipos de TI en relación con sus funciones oficiales. Este equipo pertenece a la Repartición y debe ser devuelto inmediatamente cuando lo solicite o en el momento en que un empleado sea desvinculado de la Repartición. Los usuarios pueden ser financieramente responsables del valor del equipo asignado a su cuidado si no se devuelve a la Repartición. En caso de pérdida, robo o destrucción de equipos informáticos, los usuarios deben proporcionar un informe escrito de las circunstancias que rodearon el incidente. Los usuarios pueden estar sujetos a medidas disciplinarias a instrumentarse en sumario administrativo. La Repartición tiene la discreción de no entregar dispositivos y equipos de TI a usuarios que pierdan o dañen repetidamente equipos de TI.

### 3.6 Uso de las Redes Sociales

El uso de sitios públicos de redes sociales para promover actividades gubernamentales requiere la aprobación previa por escrito de la máxima autoridad de la repartición con jerarquía no inferior a Director y notificación de las prohibiciones y responsabilidades al personal encargado de Comunicaciones. La aprobación queda a discreción de la autoridad ~~y~~ puede otorgarse previa demostración de una necesidad gubernamental y una revisión y aprobación de los términos del acuerdo de servicio por parte de la oficina de asesoria legal. La aprobación final debe definir el alcance de la actividad aprobada, incluida, entre otras, la identificación de los usuarios aprobados.
A menos que se autorice específicamente, está prohibido el uso de direcciones de correo electrónico gubernamentales en sitios públicos de redes sociales. En los casos en que los usuarios accedan a sitios de redes sociales en su propio tiempo utilizando recursos personales, deben ser sensibles a las expectativas de que se comportarán de manera responsable, profesional y segura con respecto a las referencias de la Repartición y al personal. Estas expectativas se describen a continuación.

**a. Uso de las redes sociales en el ámbito de las funciones oficiales**

La autoridad de la repartición con jerarquía no inferior a Director, debe revisar y aprobar el contenido de cualquier publicación de información pública, como comentarios de blogs, tweets, archivos de video o transmisiones, en sitios de redes sociales en nombre de la Repartición. Sin embargo, no se requiere la aprobación para publicaciones en foros públicos de soporte técnico, si la participación en dichos foros está dentro del alcance de las funciones oficiales del usuario, ha sido aprobada previamente por su supervisor y no incluye la publicación de ningún tipo de información confidencial, incluido detalles específicos de la infraestructura de TI. Además, no se requiere la aprobación para publicaciones en sitios privados de colaboración de redes sociales aprobados por la Repartición (por ejemplo, Yammer). Podrán concederse aprobaciones generales, según corresponda.

Las cuentas utilizadas para administrar la presencia de la Repartición en las redes sociales son cuentas privilegiadas y deben tratarse como tales. Estas cuentas son sólo para uso oficial y no deben utilizarse para uso personal. Las contraseñas de cuentas privilegiadas deben seguir los estándares de seguridad de la información, ser únicas en cada sitio y no deben ser las mismas que las contraseñas utilizadas para acceder a otros recursos de TI.

**b. Pautas para el uso personal de las redes sociales**

El personal debe ser consciente del hecho de que la información publicada en los sitios de redes sociales refleja claramente al individuo y también puede reflejar su vida profesional. En consecuencia, el personal debe actuar con discreción al publicar información en estos sitios y ser consciente de las posibles percepciones y respuestas a la información. Es importante recordar que una vez que la información se publica en un sitio de redes sociales, se puede capturar y utilizar de maneras no previstas originalmente. Es casi imposible retractarse, ya que a menudo permanece en copias, archivos, copias de seguridad y memoria caché.

Los usuarios deben respetar la privacidad del personal de la Repartición y no publicar ninguna información que identifique a ningún miembro del personal sin permiso (incluidos, entre otros, nombres, direcciones, fotografías, videos, direcciones de correo electrónico y números de teléfono). Los usuarios pueden ser considerados responsables de los comentarios publicados en los sitios de redes sociales.

Si un correo electrónico personal, una publicación u otro mensaje electrónico pudiera interpretarse como una comunicación oficial, se recomienda encarecidamente una exención de responsabilidad. Un descargo de responsabilidad podría ser: "Los puntos de vista y opiniones expresados son los del autor y no reflejan necesariamente los del Gobierno de la Provincia".

Los usuarios no deben utilizar sus cuentas personales de redes sociales para asuntos oficiales, a menos que lo autorice específicamente el Gobierno de la Pronvincia. Se desaconseja encarecidamente a los usuarios que utilicen las mismas contraseñas en su uso personal de los sitios de redes sociales que las utilizadas en

dispositivos gubernamentales y recursos de TI, para evitar el acceso no autorizado a los recursos si la contraseña se ve comprometida.

# Capítulo 9

# Estándar de TI: Estándar de seguridad de red inalámbrica 802.11

## 1.0 Propósito y Beneficios

El propósito de este estándar es establecer controles para redes inalámbricas 802.11 con el fin de minimizar los riesgos a la confidencialidad, integridad y disponibilidad de la información y para soportar el acceso seguro a recursos y servicios a través de redes inalámbricas.
Las redes inalámbricas 802.11 permiten a los usuarios de dispositivos inalámbricos la flexibilidad de moverse físicamente por un entorno inalámbrico manteniendo la conectividad a la red. Si bien las redes inalámbricas 802.11 están expuestas a muchos de los mismos riesgos que las redes cableadas, también están expuestas a riesgos adicionales exclusivos de las tecnologías inalámbricas. Este estándar describe los controles adicionales necesarios para el uso de redes inalámbricas.

## 2.0 Alcance

Este estándar se aplica a todas las redes inalámbricas 802.11 que almacenan, procesan, transmiten datos o se conectan a una red o sistema, incluidas las redes administradas y alojadas por terceros en nombre de la organización.
Los tipos de redes inalámbricas 802.11 abarcados incluyen:

- Internas: estas redes inalámbricas están conectadas directamente a los recursos internos de tecnología de la información y solo están disponibles para usuarios autenticados.
- Públicas (autenticadas): estas redes inalámbricas no están conectadas a recursos internos de tecnología de la información y el acceso está limitado a usuarios autenticados.
- Públicas (no autenticadas): estas redes inalámbricas no están conectadas a recursos internos de tecnología de la información y están disponibles para que cualquiera las use sin autenticación.

## 3.0 Declaración de Información

1. Las redes inalámbricas 802.11 deben seguir todos los requisitos de la Política de seguridad de la información, incluida, entre otras, una evaluación de riesgos antes de la implementación.
2. Todas las instalaciones inalámbricas deberán estar autorizadas por el MPEyM cuyos datos atravesarán la red inalámbrica.

3. La documentación del plan de seguridad, según lo exige el Estándar del ciclo de vida de desarrollo de sistemas seguros, debe incluir, como mínimo, el nombre del departamento, todas las ubicaciones de AP, todas las ubicaciones de infraestructura inalámbrica de soporte, la subred en la red cableada y el identificador de conjunto de servicios (SSID).

4. Los AP y otros dispositivos inalámbricos de soporte deben colocarse en una ubicación físicamente protegida que minimice las oportunidades de robo, daño o acceso no autorizado.

5. Se debe gestionar la cobertura de la red inalámbrica para restringir la capacidad de conectarse fuera de los límites aprobados.

6. El SSID de las redes inalámbricas 802.11 debe, si o si, cambiarse de la configuración predeterminada que tiene de fábrica.

7. El SSID no debe incluir información que indique la ubicación, tecnología o detalles del fabricante de la red inalámbrica (por ejemplo, Server-Rm-WiFi-Access, Wifi-Rm70 y Cisco-2400-WiFi). El SSID tampoco debe incluir información que indique el tipo de datos que atraviesan la red.

8. Se debe utilizar un sistema inalámbrico de detección de intrusos (IDS) en todas las redes inalámbricas internas.

9. Las redes inalámbricas públicas deben estar, como mínimo, separadas física o lógicamente de la red interna o configurada para hacer un túnel hacia un punto final seguro fuera de la red interna. El diseño debe incluirse en el plan de seguridad documentado.

10. Los esquemas de direccionamiento lógico utilizados para la red inalámbrica deben diferir de los utilizados para la red cableada para poder distinguir eficazmente las conexiones de clientes entre las dos redes.

11. Si bien se puede acceder a los servidores y recursos compartidos de información a través de una red inalámbrica, no deben conectarse directamente a una red inalámbrica.

12. APs de redes inalámbricas públicas autenticadas o internas deben configurarse para proporcionar la configuración de cifrado más segura disponible. Como mínimo, se debe utilizar acceso protegido Wi-Fi (WPA) 2 – Estándar de cifrado avanzado (AES).

13. El modo personal WPA2 no debe utilizarse para redes internas.

14. El modo personal WPA2, con el acceso protegido Wi-Fi (WPS) deshabilitado, se puede utilizar para puntos de acceso públicos autenticados que no se conectan a redes internas.

15. Los AP que utilizan frases de contraseña (como los AP configurados para usar el modo personal WPA2) deben usar frases de contraseña que cumplan con el

estándar de tokens de autenticación y deben tener al menos 14 caracteres de longitud y cambiarse como mínimo cada seis meses.

16. Las frases de contraseña utilizadas por los AP deben cambiarse desde la configuración predeterminada de fábrica.

17. No se debe poder acceder directamente a la consola de administración de la red inalámbrica desde la red inalámbrica.

18. Se debe utilizar la autenticación 802.1X, específicamente el Protocolo de autenticación extensible (EAP), para todos los dispositivos que se conectan a las redes inalámbricas internas. Los encargados de seguridad deben utilizar el método EAP-TLS siempre que sea posible. No se permite el uso de EAP ligero (LEAP) ni el uso de los siguientes mecanismos de autenticación EAP: EAP-MD5 (resumen de mensajes), EAP-OTP (contraseña de un solo uso) y EAP-GTC (tarjeta token genérica).

19. Los dispositivos cliente inalámbricos que se conectan a redes inalámbricas internas deben configurarse para validar los certificados emitidos por el servidor de autenticación durante el proceso de autenticación.

20. Los dispositivos cliente inalámbricos deben configurarse para utilizar configuraciones de privacidad de identidad durante el proceso de autenticación, cuando sea técnicamente posible.

21. Se requiere autenticación de usuario individual, de acuerdo con el Estándar de token de autenticación, para las redes inalámbricas internas.

## 4.0 Cumplimiento

Los empleados que incumplan esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y/o administrativas si correspondieren. Los no empleados, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

## 5.0 Definiciones de términos clave

| **Término** | Definición |
|---|---|
| WPA | Wi-fi Protected Access, es una tecnología de seguridad para redes del estándar WiFi, desarrollado para sanear las falencias en autenticación y encriptación de WEP. |
| WPA2 | Wi-fi Protected Access 2, es una tecnología de seguridad para redes del estándar WiFi, revisión de la WPA original, creado con el propósito de suplir algunas de las falencias del mismo. |

| | |
|---|---|
| WPA3 | Wi-fi Protected Access 2, es una tecnología de seguridad para redes del estándar WiFi, a diferencia de la anterior, registra nuevos dispositivos a través de procesos que no requieren el uso de una contraseña compartida, hacienda uso de código QR o etiquetas NFC, entre otras mejoras de seguridad. |
| WPS | WiFi Protected Setup, es un estándar de red seguro para la creación de una red domestica inalámbrica. |
| WEP | Wired Equivalent Privacy, es un sistema de cifrado para el estándar IEEE 802.11 como protocolo para redes del estándar WiFi, uno de los primeros intentos de brindar confidencialidad en las redes inalámbricas. En desuso por vulnerabilidades de seguridad. |
| SSID | Service Set Identifier, es la identificación asociada a una red de área local inalámbrica, del estándar WiFi, para que un cliente o usuario pueda diferenciarla de otras. |

## 6.0 Historial de revisiones

| Fecha | Descripción de Cambio | Crítico |
|---|---|---|
| 02/07/2024 | Draft final del documento | Alejandro Castro<br>Pablo Zalazar |

## 7.0 Documentos relacionados

Estándar de seguridad para dispositivos móviles

Estándar de cifrado

# Capítulo 10

# Estándar de IT: Política de integridad de sistemas e información

### 1.0 OBJETIVO

Garantizar que los recursos y sistemas de información de tecnología de la información (TI) se establezcan con monitoreo de la integridad del sistema para incluir áreas de preocupación como malware, fallas en aplicaciones y códigos fuente, alertas proporcionadas por la industria y solución de problemas de integridad detectados o divulgados.

### 2.0 POLÍTICA

Esta política es aplicable a todos los departamentos y usuarios de recursos y activos de TI.

1. SOLUCIÓN DE DEFECTOS
   El Departamento de TI deberá:

   a. Identificar, reportar y corregir fallas en los sistemas de información.

   b. Testear las actualizaciones de software y firmware relacionadas con la corrección de fallas para determinar su efectividad y posibles efectos secundarios antes de la instalación.

   c. Instalar actualizaciones de software y firmware relevantes para la seguridad dentro de un tiempo sugerido de 30 días desde el lanzamiento de las actualizaciones.

   d. Incorporar la corrección de fallas en el proceso de gestión de la configuración, de acuerdo con la Política de Gestión de Configuraciones.

   e. Emplear mecanismos automatizados en una frecuencia definida por la Repartición para determinar el estado de los componentes del sistema de información con respecto a la corrección de fallas.

2. PROTECCIÓN DE CÓDIGO MALICIOSO
   El Departamento de TI deberá:

a. Emplear mecanismos de protección de códigos maliciosos en los puntos de entrada y salida del sistema de información para detectar y erradicar códigos maliciosos.

b. Actualizar los mecanismos de protección de códigos maliciosos cada vez que haya nuevas versiones disponibles de acuerdo con la política y los procedimientos de gestión de configuración.

c. Configurar mecanismos de protección de código malicioso para:

   i. Realizar escaneos periódicos del sistema de información en una frecuencia definida por la Repartición y escaneos en tiempo real de archivos de fuentes externas en el punto final; puntos de entrada/salida de la red a medida que los archivos se descargan, abren o ejecutan de acuerdo con la política de seguridad.

   ii. Bloquear código malicioso, poner en cuarentena código malicioso, enviar alerta al encargado u oficial de la Seguridad de la Información, tomando las acciones pertinentes en respuesta a la detección de códigos maliciosos.

   iii. Abordar la recepción de falsos positivos durante la detección y erradicación de códigos maliciosos y el consiguiente impacto potencial en la disponibilidad del sistema de información.

3. MONITOREO DEL SISTEMA DE INFORMACIÓN
   El Departamento de TI deberá:

   a. Monitorear el sistema de información para detectar:

      i. Ataques e indicadores de posibles ataques.

      ii. Conexiones locales, de red y remotas no autorizadas.

   b. Identificar el uso no autorizado del sistema de información mediante técnicas y métodos definidos.

   c. Implementar dispositivos de monitoreo ubicaciones estratégicas dentro de la arquitectura de un sistema de información para recolectar información relevante determinada por la Repartición y en ubicaciones ad hoc dentro del sistema para rastrear tipos específicos de transacciones de interés para la Repartición.

   d. Proteger la información obtenida de las herramientas de monitoreo de intrusiones contra el acceso, modificación y eliminación no autorizados.

   e. Aumentar el nivel de actividad de monitoreo del sistema de información siempre que haya una indicación de un mayor riesgo para las operaciones y los activos,

los individuos, otras organizaciones o en base a información de aplicación de la ley, información de inteligencia u otras fuentes creíbles de información.

f. Obtener opinión legal con respecto a las actividades de monitoreo del sistema de información de acuerdo con las leyes, directivas, políticas o regulaciones nacionales y provinciales aplicables.

g. Proporcionar información de monitoreo del sistema de información al personal autorizado o unidades de gubernamentales según sea necesario.

4. ALERTAS GENERADAS POR EL SISTEMA
El Departamento de TI deberá garantizar que:

a. El sistema de información que puede generarse a partir de una variedad de fuentes, incluidos, por ejemplo, registros de auditoría o entradas de mecanismos de protección de códigos maliciosos, mecanismos de detección o prevención de intrusiones o dispositivos de protección de límites como firewalls, puertas de enlace y enrutadores, se difundirá a personal o unidades gubernamentales autorizados que tomarán las medidas adecuadas ante la(s) alerta(s).

b. Las alertas se transmitirán por teléfono, mensajes de correo electrónico o mensajes de texto, según sea necesario. El personal en la lista de notificaciones puede incluir administradores de sistemas, encargados de áreas, propietarios de sistemas o funcionarios de seguridad del sistema de información.

5. ALERTAS, AVISOS Y DIRECTIVAS DE SEGURIDAD
El Departamento de TI deberá:

a. Recibir alertas, avisos y directivas de seguridad del sistema de información de entidades externas definidas por la Repartición y el MPEyM, de forma continua.

b. Generar alertas, avisos y directivas de seguridad interna según se considere necesario.

c. Difundir alertas, avisos y directivas de seguridad para: personal o roles definidos por la Repartición, sobre elementos definidos por la Repartición dentro de la organización, organizaciones externas definidas por la Repartición.
d. Implementar las directivas de seguridad de acuerdo con los plazos establecidos, o notificar al organismo emisor el grado de incumplimiento.

6. INTEGRIDAD DEL SOFTWARE, FIRMWARE E INFORMACIÓN
El Departamento de TI deberá:

a. Emplear herramientas de verificación de integridad para detectar cambios no autorizados en software, firmware e información definidos por la Repartición;

b. Asegurar que el sistema de información realice una verificación de integridad de software, firmware e información definidos por la Repartición al inicio y/o al producirse estados de transición definidos por la Repartición o eventos relevantes para la seguridad, en una frecuencia definida por la Repartición.

c. Incorporar la detección de cambios no autorizados cambios relevantes para la seguridad definidos por la Repartición y el MPEyM en el sistema de información en la capacidad de respuesta a incidentes.

7. PROTECCIÓN CONTRA EL SPAM
El Departamento de TI deberá:

a. Emplear mecanismos de protección contra spam en los puntos de entrada y salida del sistema de información para detectar y tomar medidas ante mensajes no solicitados.

b. Actualizar los mecanismos de protección contra spam cuando haya nuevas versiones disponibles de acuerdo con la política y los procedimientos de gestión de configuración.

c. Gestionar los mecanismos de protección contra spam de forma centralizada.

d. Garantizar que los sistemas de información actualicen automáticamente los mecanismos de protección contra spam.

8. VALIDACIÓN DEL INGRESO DE INFORMACIÓN
El Departamento de TI deberá:

a. Asegurar el sistema de información:

i. Comprobar la validez de ingresos/entradas de registros de información definidas por la Repartición.

ii. Proporcionar una capacidad de anulación manual para la validación de ingresos de registros definidos por el MPEyM.

iii. Restringir el uso de la capacidad de anulación manual a solo personas autorizadas definidas por la Repartición ante el MPEyM.

iv. Auditar el uso de la capacidad de anulación manual a cargo del MPEyM.

v. Revisar y resolver errores de validación de ingresos de registros.

vi. Documentar y seguir los procedimientos correspondientes que reflejen los objetivos del sistema cuando se reciben el ingreso de registros no válidos.

9. MANEJO DE ERRORES
   El Departamento de TI deberá:

a. Asegurar el sistema de información:

   i. Generar mensajes de error que brindan información necesaria para acciones correctivas sin revelar información que pueda ser explotada por adversarios.

   ii. Revelar mensajes de error sólo al personal o roles definidos por la Repartición, y las auditorías externas facultadas a tal fin.

10. MANEJO Y RETENCIÓN DE INFORMACIÓN
    El Departamento de TI deberá:

    a. Manejar y retener información dentro del sistema de información y la información generada por el sistema de acuerdo con las leyes, directivas, políticas, regulaciones, estándares y requisitos operativos nacionales y provinciales aplicables.

11. PROTECCIÓN DE LA MEMORIA
    El Departamento de TI deberá:

    a. Asegurar que el sistema de información implemente salvaguardias de seguridad definidas por la Repartición para proteger su memoria de la ejecución de código no autorizado.

## 3.0 CUMPLIMIENTO

Los empleados que incumplan esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y/o administrativas si correspondieren. Los no empleados, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

## 4.0 EXCEPCIONES DE POLÍTICA

Las solicitudes de excepciones a esta política serán revisadas por el Director de Ciberseguridad (DC) y la Secretaría de Innovación Pública (SIP). Los departamentos que soliciten excepciones deberán proporcionar dichas solicitudes al DC/SIP. La solicitud debe indicar específicamente el alcance de la excepción junto con la justificación para otorgar la excepción, el posible impacto o riesgo asociado al otorgar la excepción, las medidas de mitigación de riesgos que debe tomar el Departamento de TI, iniciativas, acciones y un cronograma para lograrlo, el nivel mínimo de cumplimiento de las políticas aquí

establecidas. El DC/SIP revisará dichas solicitudes; consultar con el departamento solicitante.

## 5.0 FECHA DE EMISIÓN/FECHA DE REVISIÓN

| Fecha | Descripción de Cambio | Crítico |
|---|---|---|
| 05/07/2024 | Draft final del documento | Alejandro Castro<br>Pablo Zalazar |
| 11/07/2024 | Agregado de comentarios, corrección de errores. | Alejandro Castro |

## 6.0 REFERENCIA

Publicaciones especiales (SP) del Instituto Nacional de Estándares y Tecnología (NIST): NIST SP 800-53a: integridad del sistema y de la información (SI), NIST SP 800-12, NIST SP 800-40, NIST SP 800-45, NIST SP 800-83, NIST SP 800-61, NIST SP800-83, NIST SP 800-92, NIST SP 800-100, NIST SP 800-128, NIST SP 800-137, NIST SP 800-147, NIST SP 800-155

# Capítulo 11

# Estándar de IT: Política de Gestión de Configuración

### 1.0 OBJETIVO

Garantizar que los recursos de tecnología de la información (TI) estén inventariados y configurados de conformidad con las políticas, estándares y procedimientos de seguridad de TI.

### 2.0 POLÍTICA

Esta política es aplicable a todos los departamentos y usuarios de recursos y activos de TI.

1. CONFIGURACIÓN BASE
   El Departamento de TI deberá:

   a. Desarrollar, documentar y mantener bajo control de configuración, una línea base de configuraciones de los sistemas de información.

   b. Revisar y actualizar la configuración base de los sistemas de información en una frecuencia definida por la Repartición.

   c. Revisar y actualizar la configuración base del sistema de información cuando sea necesario como resultado de alguna circunstancia o evento definido por la Repartición y como parte integral de las instalaciones y actualizaciones de los componentes del sistema de información.

   d. Conservar una versión anterior de las configuraciones básicas de los sistemas de información para respaldar el rollback.

2. CONTROL DE CAMBIO DE CONFIGURACIÓN
   El Departamento de TI deberá:

   a. Determinar los tipos de cambios en el sistema de información que están controlados por la configuración.

   b. Revisar los cambios propuestos controlados por la configuración del sistema de información y aprobar o desaprobar dichos cambios teniendo en cuenta explícitamente los análisis de impacto en la seguridad.

   c. Documentar las decisiones de cambio de configuración asociadas al sistema de información.

d. Implementar cambios aprobados controlados por la configuración en el sistema de información.

e. Conservar registros de cambios controlados por la configuración en el sistema de información en un período de tiempo de cinco (5) años.

f. Auditar y revisar actividades asociadas con cambios controlados por la configuración del sistema de información.

g. Coordinar y supervisar las actividades de control de cambios de configuración a través de un órgano de control de cambios de configuración definido por la Repartición (sea interno o externo que convoca en una frecuencia que resulte adecuada a las necesidades de la Repartición) que convoca en una frecuencia definida por la Repartición, bajo condiciones de cambio de configuración definidas por la Repartición.

h. Probar, validar y documentar los cambios en el sistema de información antes de implementar los cambios en el sistema operativo.

3. ANÁLISIS DE IMPACTO EN LA SEGURIDAD
El Departamento de TI deberá:

a. Analizar los cambios en el sistema de información para determinar los posibles impactos en la seguridad antes de la implementación del cambio.

4. RESTRICCIONES DE ACCESO AL CAMBIO
El Departamento de TI deberá:

a. Definir, documentar, aprobar y hacer cumplir las restricciones de acceso físico y lógico asociadas con cambios en el sistema de información.

5. AJUSTES DE CONFIGURACIÓN
El Departamento de TI deberá:

a. Establecer y documentar los ajustes de configuración para las soluciones tecnológicas de la información empleados dentro del sistema de información utilizando listas de verificación de configuración de seguridad definidas por la Repartición que reflejen el modo más restrictivo compatible con los requisitos operativos.

b. Implementar los ajustes de configuración.

c. Identificar, documentar y aprobar cualquier desviación de los ajustes de configuración establecidos para componentes del sistema de información definidos por la Repartición en requisitos operativos definidos por la misma.

d. Monitorear y controlar los cambios en los ajustes de configuración de acuerdo con las políticas y procedimientos.

6. MÍNIMA FUNCIONALIDAD
   El Departamento de TI deberá:

   a. Configurar el sistema de información para proporcionar sólo capacidades esenciales.

   b. Revisar trimestralmente el sistema de información para identificar funciones, puertos, protocolos y servicios innecesarios y/o no seguros.

   c. Deshabilitar funciones, puertos, protocolos y servicios dentro del sistema de información que se consideren innecesarios y/o inseguros.

   d. Impedir la ejecución del programa de acuerdo con las políticas relativas al uso del programa de software y las restricciones y reglas que autorizan los términos y condiciones de uso del programa de software.

   e. Identificar programas de software no autorizados para ejecutarse en sistemas de información.

   f. Emplear una política de denegar todo y permitir por excepción para la ejecución de programas de software autorizados en el sistema de información.

   g. Revisar y actualizar la lista de programas de software autorizados anualmente.

7. INVENTARIO DE COMPONENTES DEL SISTEMA DE INFORMACIÓN
   El Departamento de TI deberá:

   a. Desarrollar y documentar un inventario de los componentes del sistema de información que:

      i. Refleja fielmente el sistema de información actual.

      ii. Incluir todos los componentes dentro del límite de autorización del sistema de información.

      iii. Esté en el nivel de granularidad que se considere necesario para el seguimiento y la presentación de informes.

      iv. Incluir información que se considere necesaria para lograr una rendición de cuentas eficaz de los componentes del sistema de información.

   b. Revisar y actualizar el inventario de componentes del sistema de información en una frecuencia definida por la Repartición.

c. Actualizar el inventario de componentes del sistema de información como parte integral de las instalaciones, remociones y actualizaciones del sistema de información.

d. Emplear mecanismos automatizados trimestralmente para detectar la presencia de componentes de hardware, software y firmware no autorizados dentro del sistema de información.

e. Tomar las siguientes acciones cuando se detecten componentes no autorizados:

    i. Deshabilitar el acceso a la red por parte de dichos componentes, o

    ii. Aislar los componentes y notificar al encargado de seguridad información y al propietario del sistema.

f. Verificar que todos los componentes dentro del límite de autorización del sistema de información no estén duplicados en otros inventarios de componentes del sistema de información.

8. PLAN DE GESTIÓN DE LA CONFIGURACIÓN
   TI deberá desarrollar, documentar e implementar un plan de gestión de la configuración para el sistema de información que:

    a. Aborde roles, responsabilidades, procesos y procedimientos de gestión de configuración.

    b. Establece un proceso para identificar elementos de configuración a lo largo del ciclo de vida de desarrollo del sistema y para gestionar la configuración de los elementos de configuración.

    c. Define los elementos de configuración para el sistema de información y coloca los elementos de configuración bajo gestión de configuración.

    d. Protege el plan de gestión de configuración contra divulgación y modificaciones no autorizadas.

9. RESTRICCIONES DE USO DEL SOFTWARE
   El Departamento de TI deberá:

    a. Utilizar el software y la documentación asociada de acuerdo con los acuerdos contractuales y las leyes de derechos de autor.

    b. Realizar un seguimiento del uso del software y la documentación asociada protegidos por licencias de cantidad para controlar la copia y distribución.

c. Controlar y documentar el uso de la tecnología de intercambio de archivos peer-to-peer (o punto a punto) para garantizar que esta capacidad no se utilice para la distribución, exhibición, ejecución o reproducción no autorizada de trabajos protegidos por derechos de autor.

10. SOFTWARE INSTALADO POR EL USUARIO
El Departamento de TI deberá:

a. Establecer políticas que regulen la instalación de software por parte de los usuarios.

b. Hacer cumplir las políticas de instalación de software controlando el acceso privilegiado y bloqueando la ejecución de archivos mediante la política aplicada por el servicio de directorio y/o la lista blanca de aplicaciones.

c. Supervisar el cumplimiento de las políticas en una frecuencia trimestral.

## 3.0 CUMPLIMIENTO

Los empleados que incumplan esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y/o administrativas si correspondieren. Los no empleados, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

## 4.0 EXCEPCIONES DE POLÍTICA

Las solicitudes de excepciones a esta política serán revisadas por el Director de Ciberseguridad (DC) y la Secretaría de Innovación Pública (SIP), y/o Encargado de Seguridad de la Información. Los departamentos que soliciten excepciones deberán proporcionar dichas solicitudes al DC/SIP. La solicitud debe indicar específicamente el alcance de la excepción junto con la justificación para otorgar la excepción, el posible impacto o riesgo asociado al otorgar la excepción, las medidas de mitigación de riesgos que debe tomar el Departamento de TI, iniciativas, acciones y un cronograma para lograrlo, el nivel mínimo de cumplimiento de las políticas aquí establecidas. El DC/SIP revisará dichas solicitudes; consultar con el departamento solicitante.

## 5.0 FECHA DE EMISIÓN/FECHA DE REVISIÓN

| Fecha | Descripción de Cambio | Crítico |
|---|---|---|
| 10/07/2024 | Draft final del documento | Alejandro Castro<br>Pablo Zalazar |
| 15/07/2024 | Revisión, corrección de errores, y agregado de comentarios. | Alejandro Castro |

## 6.0 REFERENCIA

Publicación especial (SP) del Instituto Nacional de Estándares y Tecnología (NIST): NIST SP 800-53a – Gestión de configuración (CM)

# Capítulo 12

# Estándar de TI: Estándar de Cifrado

## 1.0 Propósito y Beneficios

El cifrado es una operación criptográfica que se utiliza para mejorar la seguridad y proteger los datos electrónicos ("datos") transformando información legible (“texto sin formato”) en información ininteligible (“texto cifrado”). El cifrado es una herramienta eficaz para mitigar la amenaza del acceso no autorizado a los datos.

## 2.0 Alcance

Esta norma se aplica a todos los sistemas, que incluyen sitios web y servicios web, para los cuales la Repartición tiene responsabilidad administrativa, incluidos aquellos administrados y alojados por terceros en nombre del Gobierno de la Provincia de Jujuy.

## 3.0 Declaración de Información

La necesidad de cifrar la información se basa en su clasificación, los resultados de la evaluación de riesgos y el caso de uso.
Se debe prestar atención a las regulaciones y restricciones nacionales (por ejemplo, controles de exportación) que pueden aplicarse al uso de técnicas criptográficas en diferentes partes del mundo.
Sin perjuicio de las normas nacionales que resultaren aplicables, los productos de cifrado para la confidencialidad de los datos en reposo y en tránsito deben incorporar algoritmos aprobados por entidades nacionales y/o internacionales para el cifrado de datos. Los algoritmos de cifrado aprobados se encuentran en el Apéndice A.
Los algoritmos hash transforman un mensaje digital en una representación corta para usar en firmas digitales y otras aplicaciones para validar la integridad del mensaje.
Aunque las funciones hash como SHA 1 proporcionan una cierta cantidad de seguridad, no cumplen con todos los requisitos de seguridad para funciones hash con clave como HMAC SHA 1. Consulte FIPS 180-4 para obtener más información sobre los diferentes tipos de algoritmos hash de aplicaciones así como Apéndice A.
Los algoritmos hash se pueden utilizar para múltiples propósitos, incluidos, entre otros, firmas digitales, códigos de autenticación de mensajes, funciones de derivación de claves y funciones pseudoaleatorias.
Las funciones hash aprobadas están contenidas en Apéndice A.
Está prohibido el uso de algoritmos de cifrado/funciones hash patentados, obsoletos y criptográficamente rotos.
La información electrónica utilizada para autenticar la identidad de un individuo o proceso (es decir, PIN, contraseña, frase de contraseña) debe cifrarse cuando se almacena, transporta o transmite. Esto no incluye la distribución de un PIN, contraseña, frase de contraseña, código token, etc. de un solo uso, siempre que no se distribuya junto con ninguna otra información de autenticación (por ejemplo, ID de usuario).

El plan de seguridad de un sistema debe incluir documentación que muestre una revisión adecuada de las metodologías y productos de cifrado. Esto demostrará la debida diligencia al elegir un método o producto que haya recibido una revisión positiva sustancial por parte de analistas externos acreditados.

### 3.1 Datos en Tránsito

Se requiere cifrado para los datos en tránsito en las siguientes situaciones:

1. Cuando se transmite información electrónica de identificación personal (PII) (incluidos, entre otros, correo electrónico, protocolo de transferencia de archivos (FTP), mensajería instantánea, fax electrónico, voz sobre protocolo de Internet (VoIP), etc.).

2. Cuando el cifrado de datos en tránsito esté prescrito por ley o reglamento.

3. Al conectarse a las redes internas a través de una red inalámbrica.

4. Al acceder de forma remota a las redes o dispositivos internos de una Repartición a través de una red compartida (por ejemplo, Internet) o personal (por ejemplo, Bluetooth, infrarrojos). Esto no se aplica al acceso remoto a través de una conexión dedicada punto a punto administrada por una Repartición.

5. Cuando los datos se transmiten con el sitio web público y/o los servicios web de una entidad, se les exige utilizar el Protocolo seguro de transferencia de hipertexto (HTTPS) en lugar del Protocolo de transferencia de hipertexto (HTTP) cuando sea técnicamente posible. Los sitios web públicos deben utilizar HTTP Strict Transport Security (HSTS), redirigiendo automáticamente las solicitudes HTTP a sitios web HTTPS cuando sea técnicamente posible. La compatibilidad mínima del navegador se enumera en el Apéndice B.

Los métodos de cifrado adecuados para los datos en tránsito incluyen, entre otros, Transport Layer Security (TLS) 1.2 o posterior, Secure Shell (SSH) 2.0 o posterior, Wi-Fi Protected Access (WPA) versión 2 o posterior (con WiFi Protected Access). Configuración deshabilitada) y redes privadas virtuales (VPN) cifradas. Los componentes deben configurarse para admitir los conjuntos de cifrado más potentes posibles. Los cifrados que no cumplan con este estándar deben desactivarse.

### 3.2 Los Datos en Reposo

Se requiere cifrado para los datos en reposo, de la siguiente manera:

1. Para los sistemas enumerados a continuación:

    a. Escritorios que acceden o contienen información de identificación personal (PII);

    b. Almacenes de datos (incluidos, entre otros, bases de datos y archivos compartidos) que contienen PII;

    c. Todos los dispositivos móviles, ya sea emitidos por la Repartición o de terceros, que accedan o contengan cualquier información de la Provincia; y

d. Todos los dispositivos de almacenamiento portátiles que contengan cualquier información de la Provincia.

2. Cuando la información PII electrónica se transporta o almacena fuera de las instalaciones del Gobierno de la Provincia.

Se requiere cifrado de disco completo para todas las computadoras portátiles emitidas por alguna Repartición que acceden o contienen información del Gobierno de la Provincia. Los productos de cifrado de disco completo deben utilizar autenticación previa al arranque que utiliza el Módulo de plataforma segura (TPM) del dispositivo o el arranque seguro de la interfaz de firmware extensible unificada (UEFI).
Para mitigar los ataques contra las claves de cifrado, cuando se encuentren fuera de las instalaciones de la Repartición, las computadoras portátiles y las computadoras portátiles de terceros que accedan o contengan PII deben apagarse (es decir, apagarse o hibernarse) cuando estén desatendidas.
La entidad debe contar con un proceso o procedimiento para confirmar que los dispositivos y medios se hayan cifrado exitosamente utilizando al menos uno de los siguientes, enumerados en orden preferido:

1. aplicación automatizada de políticas;

2. sistema de inventario automatizado; o

3. mantenimiento de registros manuales.

### 3.3 Gestión de Claves

La entidad debe garantizar que se establezca un entorno seguro para proteger las claves criptográficas utilizadas para cifrar y descifrar la información. Las claves deben distribuirse y almacenarse de forma segura.
El acceso a las claves debe restringirse únicamente a las personas que tengan una necesidad gubernamental de acceder a las claves.
Las claves no cifradas no deben almacenarse con los datos que cifran. Las claves estarán protegidas con un token de autenticación que se ajuste al nivel de seguridad identificado.
El compromiso de una clave criptográfica haría que toda la información cifrada con esa clave se considere no cifrada. Si se descubre un compromiso, se debe generar y utilizar una nueva clave para continuar con la protección de la información cifrada. Se deben evaluar circunstancias específicas para determinar si se requiere una notificación de incumplimiento.
Las claves de cifrado y sus productos de software asociados deben conservarse durante la vida útil de los datos archivados que se cifraron con ese producto.

## 4.0 Cumplimiento

Los empleados que incumplan esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y/o administrativas si correspondieren. Los no empleados, incluidos, entre otros, los contratistas, pueden

estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

## 5.0 Definiciones de términos clave

| **Término** | Definición |
|---|---|
| | |

## 6.0 Historial de revisiones

| **Fecha** | **Descripción de Cambio** | **Crítico** |
|---|---|---|
| | | |

## 7.0 Documentos relacionados

Publicación 140-2 del Estándar Federal de Procesamiento de Información (FIPS) del NIST

Publicación 198-1 del Estándar Federal de Procesamiento de Información (FIPS) del NIST

Publicación 180-4 del Estándar Federal de Procesamiento de Información (FIPS) del NIST

Publicación especial del NIST 800-107, revisión 1, recomendación para aplicaciones que utilizan algoritmos hash aprobados

APÉNDICE A

Los algoritmos **Secure Hash Algorithms (SHA)** son una familia de funciones hash criptográficas diseñadas por el **National Institute of Standards and Technology (NIST)** para proporcionar integridad y autenticidad en la transmisión y almacenamiento de datos. Estas funciones generan un valor hash fijo a partir de datos de entrada, actuando como una "huella digital" del mensaje o documento.

**Principales Algoritmos SHA:**

1. **SHA-1:** Genera un hash de 160 bits. Fue ampliamente utilizado en aplicaciones de seguridad como SSL/TLS, firmas digitales y certificados digitales.
2. **SHA-224, SHA-256, SHA-384 y SHA-512:** Forman parte de la familia SHA-2, con hashes de 224, 256, 384 y 512 bits, respectivamente. Estos algoritmos mejoran la seguridad frente a colisiones y ataques de preimagen.

**Deprecación de SHA-1 por NIST:**

**SHA-1** fue desarrollado en 1993 como parte de la primera generación de algoritmos de hash seguro. Aunque inicialmente fue seguro, con el tiempo se descubrieron vulnerabilidades criptográficas significativas que lo hicieron susceptible a ataques de colisión.

**Deprecación de SHA-1:**

- **Fecha de deprecación:** En 2011, NIST declaró que **SHA-1** debía ser reemplazado por SHA-2 para todas las aplicaciones nuevas y que su uso debía ser descontinuado gradualmente. A partir de **2017**, NIST retiró formalmente el soporte para SHA-1 en la mayoría de las aplicaciones.
- **Fecha de retiro**: NIST anuncia el retiro de SHA-1 y recomienda que se migre a SHA-2 o SHA-3 tan pronto como sea posible. La fecha límite es el 31 de diciembre, 2030.

| Tipo de HASH | Longitud del HASH | Características | Casos de Uso |
|---|---|---|---|
| **MD5** | 128 bits | - Rápido. | - Comprobación de integridad de archivos (no recomendado para seguridad). |
| | | - Vulnerable a colisiones y ataques de preimagen. | |
| **SHA-1** | 160 bits | - Mayor longitud que MD5. | - Firmas digitales (obsoleto). |
| | | - Vulnerable a colisiones. | - Certificados SSL/TLS (descontinuado). |
| **SHA-224** | 224 bits | - Parte de la familia SHA-2. | - Usado en sistemas con limitaciones de almacenamiento. |
| | | - Menor tamaño que SHA-256, pero similar en seguridad. | - Certificados digitales. |
| **SHA-256** | 256 bits | - Alta seguridad. | - Firmas digitales. |
| | | - Amplio uso en criptografía moderna. | - Certificados SSL/TLS. |
| | | | - Criptomonedas como Bitcoin. |
| **SHA-384** | 384 bits | - Mayor seguridad debido a la longitud del hash. | - Usado en sistemas que requieren alta seguridad. |
| | | - Parte de SHA-2. | - Protección de datos críticos. |
| **SHA-512** | 512 bits | - Máxima seguridad en la familia SHA-2. | - Certificados digitales. |
| | | - Adecuado para datos altamente sensibles. | - Seguridad en comunicaciones críticas. |
| | | | - Protección de grandes volúmenes de datos. |
| **SHA-3** | Variable (224, 256, 384, 512 bits) | - Diferente diseño a SHA-2. | - Aplicaciones que requieren resistencia cuántica. |
| | | - Alta resistencia a ataques avanzados. | - Reemplazo potencial para SHA-2 en el futuro. |

| **Algoritmo** | **Longitud mínima de clave** | **Caso de uso** |
|---|---|---|
| AES | 128 | Cifrado de datos |
| RSA | 2048 | Firmas digitales<br>Cifrado de clave pública |
| ECDSA | 256 | Firma digital<br>Cifrado de clave pública |
| sha | 256 | hash |
| HMAC SHA 1 | 112 | Código de autenticación de mensaje hash con clave |

# Capítulo 13

# Estándar de TI: Estándar de Registro de Seguridad

## 1.0 Propósito y Beneficios

Los registros compilan datos para que los sistemas y las redes puedan monitorearse adecuadamente, mantener el uso para fines autorizados y el conocimiento del entorno operativo, incluida la detección de indicios de problemas de seguridad.
Este estándar define los requisitos para la generación, gestión, almacenamiento, eliminación, acceso y uso de registros de seguridad. Los registros de seguridad son generados por muchas fuentes, incluido el software de seguridad, como software antivirus, firewalls y sistemas de prevención y detección de intrusiones; sistemas operativos en servidores, estaciones de trabajo y equipos de red; bases de datos y aplicaciones.

## 2.0 Declaración de información

Los registros deben generarse en sistemas y redes de tecnología de la información (TI). Debido a la naturaleza de los datos contenidos en los registros de seguridad (por ejemplo, contraseñas, contenido de correo electrónico), se consideran información de identificación personal (PII) y deben protegerse con controles para una confidencialidad e integridad altas.

## 2.1 Generación de Registros Inicial

a. Todos los hosts y equipos de red deben generar registros de seguridad para todos los componentes (p. ej., sistema operativo, servicio, aplicación).

b. Todos los eventos de seguridad (Apéndice A) debe registrarse y debe configurarse para capturar niveles significativos de detalle para indicar actividad.

## 2.2 Administración de Registros

a. Todos los hosts y equipos de red deben emitir alertas sobre fallas en el procesamiento de registros de seguridad, como errores de software/hardware, fallas en los mecanismos de captura de registros y capacidad de almacenamiento de registros que se alcanza o excede. Todas las alertas deben ser lo más cercanas posible al tiempo real.

b. Cuando el almacenamiento de registros no rotativo alcanza el 90 % de su capacidad, se debe emitir una advertencia.

## 2.3 Consolidación de Registros

a. La información relacionada con la seguridad de todos los sistemas, con excepción de las estaciones de trabajo individuales, debe transferirse a una infraestructura de registro consolidada. Los sistemas que ejecutan sistemas operativos de estaciones de trabajo que se utilizan para servicios compartidos, como almacenamiento de archivos compartidos o servicios web, también deben cumplir estos requisitos.

b. Todas las estaciones de trabajo deben tener la capacidad de transferir registros a una infraestructura de registros consolidada, si es necesario.

c. Los datos de registro deben transferirse en tiempo real desde hosts individuales a una infraestructura de registro consolidada. Cuando no sea posible la transferencia en tiempo real, los datos deben transferirse desde los hosts individuales a una infraestructura de registro consolidada tan rápido como lo permita la tecnología.

d. Las entidades deberán establecer procesos para el establecimiento, operación y, según corresponda, integración de sistemas de gestión de registros.

## 2.4 Almacenamiento y Eliminación de Registros

a. Dentro de la infraestructura de registros consolidada, los registros deben mantenerse y estar disponibles durante un mínimo de 90 días. Según los requisitos de la entidad, incluidas las necesidades legales o de auditoría, es posible que sea necesario conservar los registros durante un período de tiempo más largo.

b. Los datos de registro deben eliminarse de forma segura (tanto a nivel del sistema como de infraestructura) de conformidad con el Estándar de desinfección/eliminación segura.

c. Los sistemas que recopilan registros, ya sean locales o consolidados, deben mantener suficiente espacio de almacenamiento para cumplir con los requisitos mínimos tanto para los registros fácilmente disponibles como para los retenidos. La planificación del almacenamiento debe tener en cuenta las ráfagas de registros o los aumentos en los requisitos de almacenamiento que podrían razonablemente esperarse como resultado de problemas del sistema, incluida la seguridad.

d. Se debe implementar un proceso para atender las solicitudes de preservación de registros, como un requisito legal para evitar la alteración y destrucción de registros particulares (por ejemplo, cómo se deben marcar, almacenar y proteger los registros afectados).

e. Es necesario preservar la integridad de los registros para la infraestructura de registros consolidados, como almacenar registros en medios de escritura única o generar resúmenes de mensajes para cada archivo de registro.

### 2.5 Acceso y Uso de Registros

a. Los datos de registro deben analizarse inicialmente lo más cerca posible del tiempo real.

b. El acceso a los sistemas de gestión de registros debe registrarse y debe limitarse a personas con una necesidad específica de acceso a los registros. El acceso a los datos de registro debe limitarse a los conjuntos de datos específicos apropiados para las necesidades gubernamentales.

c. Deben existir procedimientos para gestionar eventos inusuales. La respuesta debe ser proporcional a la criticidad del sistema, la sensibilidad de los datos y los requisitos reglamentarios.

## 3.0 Cumplimiento

Los empleados que incumplan esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y/o administrativas si correspondieren. Los no empleados, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

## 4.0 Historial de revisiones

| Fecha | Descripción de Cambio | Crítico |
|---|---|---|
| | | |

## 5.0 Documentos relacionados

Publicación especial del NIST 800-92, Guía para la gestión de registros de seguridad informática

Los eventos de seguridad que deben registrarse para todos los sistemas incluyen, entre otros:

Eventos de autenticación exitosos y fallidos que incluyen, entre otros:

- inicio/cierre de sesión del sistema;
- cuenta o ID de usuario;
- cambio de contraseña;
- el tipo de evento;
- una indicación del éxito o fracaso del evento;
- la fecha y hora del evento; y
- Identificación de la fuente del evento, como ubicación, direcciones IP, ID del terminal u otros medios de identificación.

Los eventos de acceso fallido a recursos se registrarán para incluir como mínimo:

- cuenta o ID de usuario;
- el tipo de evento;
- una indicación del evento;
- la fecha y hora del evento;
- el recurso; y
- identificación de la fuente del evento, como ubicación, direcciones IP, identificación del terminal u otros medios de identificación.

Operaciones privilegiadas exitosas y no exitosas que incluyen, entre otras:

- uso de cuentas privilegiadas del sistema;
- el sistema arranca y se detiene;
- accesorios y desmontajes de hardware;
- alertas y mensajes de error de gestión de sistemas y redes; y
- eventos de seguridad: administración de cuentas/grupos y cambios de políticas.

Acceso exitoso y no exitoso a archivos de registro que incluyen, entre otros:

- cuenta o ID de usuario;
- el tipo de evento;
- una indicación del éxito o fracaso del evento;

- la fecha y hora del evento; y
- identificación de la fuente del evento, como ubicación, dirección IP, ID de terminal u otros medios de identificación.

La mayoría de los servidores web ofrecen la opción de almacenar archivos de registro en el formato de registro común o en un formato de registro extendido. El formato de registro extendido registra más información que el formato de archivo de registro común. Cuando sea técnicamente posible, los servidores web deben utilizar el formato de registro extendido. El formato de registro extendido agrega información de registro valiosa a su archivo de registro para que pueda determinar de dónde provienen los mensajes, quién envía el mensaje y agrega información al archivo de registro que sería necesaria para rastrear un ataque.

Para los sistemas identificados como críticos según una evaluación de riesgos o sistemas que aún no han sido clasificados, además de lo anterior, se registrarán eventos exitosos de acceso a recursos para incluir como mínimo:

- cuenta o ID de usuario;
- el tipo de evento;
- una indicación del evento;
- la fecha y hora del evento;
- el recurso; y
- identificación de la fuente del evento, como ubicación, direcciones IP, identificación del terminal u otros medios de identificación.

# Capítulo 14

# Estándar de TI: Codificación Segura

## 1.0 Propósito y Beneficios

Las organizaciones gubernamentales sufren constantes ciberataques que intentan explotar las vulnerabilidades de los sistemas informáticos y, por tanto, amenazan la confidencialidad, la integridad y la disponibilidad de la información. Una gran cantidad de vulnerabilidades que se explotan con éxito se deben a debilidades en la codificación del software y fallas en la implementación de la codificación.
El objetivo de este estándar de codificación es garantizar que el código escrito sea resistente a amenazas de alto riesgo y evitar la aparición de los errores de codificación más comunes que crean vulnerabilidades graves en el software. Si bien es imposible escribir código que sea completamente inmune a todos los posibles ataques, la implementación de estos estándares de codificación en todos los sistemas de información reducirá significativamente el riesgo de divulgación, alteración o destrucción de información debido a vulnerabilidades del software.

## 2.0 Declaración de información

Según la Política de seguridad de la información, todo el software escrito o implementado en sistemas debe incorporar prácticas de codificación segura, para evitar la aparición de vulnerabilidades de codificación comunes y ser resistente a amenazas de alto riesgo, antes de implementarse en producción.

Los elementos enumerados en este estándar no son una lista exhaustiva de ataques de alto riesgo y errores de codificación comunes, sino más bien una lista de los más dañinos y generalizados. Por lo tanto, el código escrito debe contener controles de mitigación no solo para los elementos específicamente articulados en el estándar a continuación, sino también para cualquier amenaza de riesgo medio y alto que se identifique durante el ciclo de vida de un sistema.

Las amenazas de alto riesgo incluyen, entre otras:

1. Inyección de código;
2. Secuencias de comandos entre sitios (XSS);
3. Falsificación de solicitudes entre sitios (CSRF);
4. Fuga de información y manejo inadecuado de errores;
5. Autenticación faltante para función crítica;
6. Falta de cifrado de datos confidenciales;
7. Redirección de URL a un sitio que no es de confianza ("Redirección abierta").

Como mínimo, el código debe eliminar o mitigar las amenazas identificadas en la versión actual del Open Web Application Security Project (OWASP) Los 10 riesgos de seguridad de aplicaciones más críticos ('OWASP Top 10') y la Enumeración de debilidades comunes (CWE)/SANS Los 25 errores de software más peligrosos ("CWE/SANS Top 25").

Tanto OWASP como CWE/SANS reeditan periódicamente sus respectivas listas en función de cambios en los patrones de vulnerabilidad y explotación. Los desarrolladores deben estar al tanto de las actualizaciones de estas listas e incorporar nuevas recomendaciones.

Se requiere el uso de bibliotecas de control de seguridad y API comunes, que hayan sido sometidas a pruebas de seguridad, para garantizar un enfoque coherente que minimice los defectos y evite la explotación. Cuando estén disponibles, se deben utilizar bibliotecas o API disponibles públicamente o proporcionadas por proveedores, a menos que haya un caso de negocio desarrollado y una excepción otorgada por el Oficial de Seguridad de la Información (ISO)/representante de seguridad designado para desarrollar una biblioteca personalizada.

Para prevenir defectos o detectarlos y eliminarlos tempranamente, logrando así beneficios significativos en costos y cronograma para la Repartición, se debe verificar el código en busca de errores durante el desarrollo y mantenimiento.

Las entidades deben verificar que el modelo de garantía de software utilizado por el proveedor esté en línea con este estándar a través de garantías del proveedor, pruebas de seguridad y/o requisitos contractuales.

## 3.0 Cumplimiento

Los empleados que violen esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y/o administrativas si correspondieren. Los no empleados, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

## 4.0 Historial de revisiones

| Fecha | Descripción de Cambio | Crítico |
|---|---|---|
| 29-07-24 | Documento inicial, primera revisión. | Alejandro Castro, Pablo Zalazar |

## 5.0 Documentos relacionados

Open Web Application Security Project (OWASP) Los 10 riesgos de seguridad de aplicaciones más críticos ('OWASP Top 10')

Hojas de trucos para desarrolladores del Proyecto abierto de seguridad de aplicaciones web (OWASP)

API de seguridad empresarial del Proyecto abierto de seguridad de aplicaciones web (OWASP)

Enumeración de debilidades comunes (CWE)/SANS Top 25 de los errores de software más peligrosos 'CWE/SANS Top 25')

Lista de enumeración de debilidades comunes (CWE)

Estándares de codificación segura CERT del Instituto de Ingeniería de Software Carnegie Mellon

# Capítulo 15

# Estándar de TI: Estándar Configuración Segura

## 1.0 Propósito y Beneficios

El propósito de esta norma es establecer configuraciones de referencia para los sistemas de información que son propiedad y/u operados por la Repartición. La implementación efectiva de este estándar maximizará la seguridad y minimizará el riesgo potencial de acceso no autorizado a la información y la tecnología.

## 2.0 Alcance

Esta norma se aplica a todos los sistemas de información que son propiedad de la Repartición y/u operados por ella o en nombre de ella. Los sistemas de laboratorio, como los utilizados para investigación o análisis forense digital, pueden requerir una consideración especial; sin embargo, este estándar debe aplicarse de manera obligatoria, a menos que hacerlo inhiba las funciones principales de estos sistemas o no sea técnicamente factible.

## 3.0 Declaración de Información

Se deben utilizar perfiles de configuración segura estándar, basados en una o más de las pautas de consenso de la industria que se enumeran a continuación, además de las pautas de seguridad más recientes del proveedor. Las modificaciones al perfil deben basarse en la necesidad gubernamental, la política o el cumplimiento de estándares, desarrollarse en consulta con el Oficial de Seguridad de la Información/Encargado de seguridad designado, documentarse y conservarse para fines de auditoría.

Directrices de consenso de la industria

- Puntos de referencia del Centro de Seguridad de Internet (CIS)
- Programa de lista de verificación nacional del Instituto Nacional de Ciencia y Tecnología (NIST)

La configuración inicial, la instalación del software y la configuración de seguridad de los nuevos sistemas deben realizarse en un entorno seguro aislado de otros sistemas operativos con protocolos de comunicación mínimos habilitados.

Los cambios en las configuraciones se identifican, proponen, revisan, analizan formalmente para determinar el impacto en la seguridad, se prueban y aprueban antes de su implementación de acuerdo con los procedimientos de gestión de cambios. Las personas que realizan análisis de impacto en la seguridad poseen las habilidades y la experiencia técnica necesarias para analizar los cambios en los sistemas de información y las ramificaciones de seguridad asociadas.

Las entidades deben mantener planes de gestión de la configuración que definan procesos y procedimientos detallados sobre cómo se utiliza la gestión de la configuración para respaldar las actividades seguras del ciclo de vida del desarrollo del sistema a nivel del sistema de información. Los planes de gestión de la configuración normalmente se desarrollan durante la fase de desarrollo/adquisición del ciclo de vida de desarrollo del sistema seguro.

Debe existir un proceso de monitoreo de configuración para identificar componentes del sistema no descubiertos o no documentados, configuraciones incorrectas, vulnerabilidades y cambios no autorizados.

## 4.0 Cumplimiento

Los empleados que violen esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y/o administrativas si correspondieren. Los no empleados, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

## 5.0 Historial de revisiones

| Fecha | Descripción de Cambio | Crítico |
|---|---|---|
| | | |

## 6.0 Documentos relacionados

Instituto Nacional de Estándares y Tecnología (NIST) 800-128, Guía para la gestión de la configuración de sistemas de información centrada en la seguridad

# Capítulo 16

# Estándar de TI: Estándar Gestión de Parches

## 1.0 Propósito y Beneficios

La gestión de parches de seguridad (administración de parches) es una práctica diseñada para prevenir de forma proactiva la explotación de las vulnerabilidades de TI que existen dentro de una organización. Al aplicar actualizaciones (parches) de software o firmware relacionados con la seguridad a los sistemas de TI aplicables, el resultado esperado es reducir el tiempo y el dinero dedicados a lidiar con exploits al reducir o eliminar la vulnerabilidad relacionada.

## 2.0 Alcance

Este estándar se relaciona específicamente con las vulnerabilidades que pueden abordarse mediante una actualización de software o firmware (parche) y se aplica a todo el software utilizado en los sistemas de la Repartición. Se debe seguir el Estándar de Escaneo de Vulnerabilidades para conocer los requisitos para abordar las vulnerabilidades sin parches.

## 3.0 Declaración de Información

1. Las Reparticiones deben asignar a un individuo o grupo dentro de las operaciones de TI para que sea responsable de la gestión de parches.

2. Si se subcontrata la gestión de parches, deben existir acuerdos de nivel de servicio que aborden los requisitos de este estándar y describan las responsabilidades para la aplicación de parches. Si el parcheo es responsabilidad del tercero, las entidades deben verificar que se hayan aplicado los parches.

3. Debe existir un proceso para gestionar los parches. Este proceso debe incluir lo siguiente:

    - Monitorear fuentes de seguridad (Apéndice A) para vulnerabilidades, corrección con y sin parches y amenazas emergentes;
    - Supervisar la distribución de parches, incluida la verificación de que se esté siguiendo un procedimiento de control de cambios;
    - Pruebas de estabilidad e implementación de parches; y
    - Utilizando una herramienta de distribución de gestión de parches centralizada y automatizada, siempre que sea técnicamente posible, que:
        - mantiene una base de datos de parches;
        - implementa parches en los dispositivos; y

- verifica la instalación de parches.

4. Debe existir una separación adecuada de funciones para que las personas que verifican la distribución de parches no sean las mismas que distribuyen los parches.

5. De acuerdo con la Política de Seguridad de la Información, todas las entidades deben mantener un inventario de activos de hardware y software. La gestión de parches debe incorporar todos los activos de TI instalados.

6. Se debe priorizar la gestión de parches en función de la gravedad de la vulnerabilidad que aborda el parche. En la mayoría de los casos, las clasificaciones de gravedad se basan en el Sistema de puntuación de vulnerabilidad común (CVSS). Una puntuación CVSS de 7 a 10 se considera una vulnerabilidad de alto impacto, una puntuación CVSS de 4 a 6,9 se considera una vulnerabilidad de impacto moderado y una CVSS de 0 a 3,9 se considera una vulnerabilidad de bajo impacto.

7. En la medida de lo posible, el proceso de aplicación de parches debe seguir el cronograma contenido en la siguiente tabla:

| Impacto/Severidad | Parche iniciado | Parche completado |
|---|---|---|
| Alto | Dentro de las 24 horas posteriores al lanzamiento del parche | Dentro de 1 semana del lanzamiento del parche |
| Medio | Dentro de 1 semana del lanzamiento del parche | Dentro de 1 mes desde el lanzamiento del parche |
| Bajo | Dentro de 1 mes desde el lanzamiento del parche | Dentro de los 2 meses posteriores al lanzamiento del parche, a menos que ISO determine que se trata de un riesgo insignificante para el medio ambiente. |

8. Si la aplicación de parches no se puede completar en el plazo indicado en la tabla anterior, se deben implementar controles de compensación dentro de los plazos anteriores y se debe seguir el proceso de excepción.

9. Si un parche requiere reiniciar para su instalación, el reinicio debe realizarse dentro de los plazos descritos anteriormente.

## 4.0 Cumplimiento

Los empleados que incumplan esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y/o administrativas si correspondieren. Los no empleados, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

## 5.0 Definiciones de términos clave

| Fecha | Descripción de Cambio |
|---|---|
| Exploit | Un exploit es cualquier ataque que aprovecha las vulnerabilidades de las aplicaciones, las redes, los sistemas operativos, o el hardware. |
| CVSS SIG | Es un grupo de expertos que trabajan sobre el estándar CVSS, que es una forma de puntuar/clasificar la severidad de una vulnerabilidad. |

## 6.0 Historial de revisiones

| Fecha | Descripción de Cambio | Crítico |
|---|---|---|
| | | |

## 7.0 Documentos relacionados

Instituto Nacional de Estándares y Tecnología, Publicación especial 800-40, Guía de tecnologías de gestión de parches empresariales

Sistema de puntuación de vulnerabilidad común

Estándar de escaneo de vulnerabilidades

# Capítulo 17

# Estándar de TI: Estándar Escaneo de vulnerabilidades

## 1.0 Propósito y Beneficios

Las Reparticiones utilizan herramientas automatizadas para escanear sistemas, dispositivos informáticos y de red, aplicaciones web y códigos de aplicaciones. Los resultados de estos análisis ayudan a informar al Ministerio de Planificación Estratégica y Modernización y a los administradores del sistema sobre vulnerabilidades conocidas y potenciales.
La gestión de vulnerabilidades es un proceso mediante el cual las vulnerabilidades identificadas mediante el escaneo se rastrean, evalúan, priorizan y gestionan hasta que se remedian o se resuelven adecuadamente. La gestión de las vulnerabilidades identificadas durante los análisis garantiza que se tomen las medidas adecuadas para reducir la posibilidad de que estas vulnerabilidades sean explotadas y, por lo tanto, reducir el riesgo de comprometer la confidencialidad, integridad y disponibilidad de los activos de información.

## 2.0 Declaración de información

Según la Política de seguridad de la información, todos los sistemas deben escanearse en busca de vulnerabilidades. Además, cada sistema debe estar inventariado y tener asignada una responsabilidad individual o grupal para el mantenimiento y la administración.

## 2.1 Tipos de exploraciones

El tipo de análisis de vulnerabilidad apropiados para un objetivo determinado depende del tipo de objetivo (es decir, hardware, software, código fuente) y de la ubicación del objetivo (es decir, interno o externo a la red). La siguiente tabla enumera los tipos de análisis de vulnerabilidades requeridos por este estándar.

4

| Tipo | Descripción |
|---|---|
| **Escaneo de infraestructura externa** | Escaneos del perímetro de las redes o de cualquier infraestructura alojada disponible externamente para identificar posibles vulnerabilidades en la infraestructura de TI accesible a Internet. |
| **Infraestructura interna Escanear** | Escaneos de la infraestructura de TI en redes protegidas o cualquier infraestructura alojada para identificar posibles vulnerabilidades. |
| **Escaneo de aplicaciones web “lite”** | Escaneos superficiales no autenticados de aplicaciones web de producción externas para identificar vulnerabilidades de seguridad. |
| **Escaneo en profundidad de aplicaciones web** | Al momento de implementación, se debe escanear en profundidad con autenticación de las aplicaciones web para identificar vulnerabilidades de seguridad. |
| **Análisis del código fuente de la aplicación** | Durante el desarrollo de software se deben ejecutar escaneos del código fuente de la aplicación para identificar problemas en el código que podrían causar posibles vulnerabilidades. |

## 2.2 Escaneo

Las Reparticiones son responsables de confirmar que se realizan análisis de vulnerabilidades. Las Reparticiones deben utilizar una herramienta de escaneo aprobada por la ISO/encargados de seguridad designado. Cualquier herramienta de escaneo aprobada debe poder proporcionar sugerencias de solución y asociar un valor de gravedad a cada vulnerabilidad descubierta en función del impacto relativo de la vulnerabilidad en el sistema afectado.

Según el Estándar de clasificación de la información, los informes de escaneo se clasifican con confidencialidad e integridad moderadas y deben protegerse como tales. Las Reparticiones deben proporcionar todas las direcciones IP externas y localizadores uniformes de recursos (URL) para todas las aplicaciones web externas a los encargados de seguridad designados/ISO.

Los administradores de redes y sistemas deben proporcionar acceso suficiente para permitir que el motor de escaneo de vulnerabilidades explore todos los servicios proporcionados por el sistema. Ningún dispositivo conectado a la red deberá configurarse específicamente para bloquear los escaneos de vulnerabilidades de los motores de escaneo autorizados.
Los análisis se deben realizar dentro del ciclo de vida de desarrollo del sistema (consultar el estándar relacionado) en entornos previos a la implementación, cuando se implementan en el entorno de implementación de destino y periódicamente a partir de entonces, como se especifica a continuación:

a. Los análisis previos a la implementación se realizan antes de mover el sistema o la aplicación web al entorno de implementación de destino:

    1. Todos los sistemas deben someterse a un escaneo de infraestructura interna autenticado, cuando sea técnicamente factible o necesario, antes de implementarse en el entorno de implementación de destino. Cualquier vulnerabilidad de infraestructura descubierta debe ser remediada o determinada como un falso positivo o un riesgo insignificante por el Oficial de Seguridad de la Información (ISO)/encargado de seguridad designado, antes de implementar el sistema para el uso previsto.

    2. Cuando el código fuente está disponible, las aplicaciones deben someterse a un escaneo del código fuente antes de que el código actualizado pase al entorno de implementación de destino si ha habido un cambio en el código de la aplicación.

    3. Los análisis deben autenticarse cuando la aplicación requiere autenticación antes de implementarse en el entorno de implementación de destino o en un entorno al que se pueda acceder externamente. Cuando se requiere autenticación para acceder a la aplicación, los análisis deben ejecutarse con acceso autenticado en cada nivel de acceso (por ejemplo, usuario, administrador) admitido por la aplicación, excepto cuando las limitaciones de la herramienta impidan el análisis autenticado. Cualquier vulnerabilidad de la aplicación web descubierta debe ser remediada o determinada como un falso positivo o un riesgo insignificante por parte del encargado de seguridad designado o del ISO, antes de colocar el sistema en el entorno de implementación de destino.

    4. Cualquier sistema o aplicación implementada en su entorno de implementación objetivo con vulnerabilidades no remediadas debe tener un plan de remediación formal y la aprobación documentada del ejecutivo responsable de la gestión de riesgos o su designado.

b. Los escaneos de implementación ocurren la primera vez que un sistema o aplicación web se mueve a su entorno de implementación de destino:

    1. Los sistemas deben escanearse inmediatamente después de colocarse en el entorno de implementación de destino con un escaneo de infraestructura interna autenticado, cuando sea técnicamente factible o necesario. Si se

puede acceder al sistema desde Internet o una red externa, entonces el sistema debe escanearse con un escaneo de infraestructura externa.

2. Las aplicaciones web deben escanearse dentro del primer mes de su colocación en el entorno de implementación de destino. Si es posible, se requiere un análisis en profundidad de la aplicación web autenticado, pero como mínimo se requiere un análisis "lite" de la aplicación web. Se deben considerar la sensibilidad y criticidad de la aplicación al determinar el cronograma para el escaneo de implementación inicial.

c. Escaneos recurrentes: después del escaneo inicial en el entorno de implementación de destino, la frecuencia de los escaneos debe ocurrir de acuerdo con la clasificación de riesgo del sistema o la aplicación (consulte la Tabla 2).

1. Al realizar análisis de infraestructura interna en sistemas creados con una imagen compartida, como estaciones de trabajo, los análisis se pueden ejecutar en una muestra de sistemas, pero el conjunto de muestras debe variar de un análisis a otro.

2. Las aplicaciones web en producción deben someterse a análisis recurrentes. Como mínimo, las aplicaciones web en producción deben someterse a análisis "lite" recurrentes.

3. Todas las vulnerabilidades encontradas durante los análisis deben abordarse según lo establecido en sección de remediación abajo.

### 2.3 Determinar la clasificación de riesgo y la frecuencia de los escaneos

El riesgo que las vulnerabilidades representan para los sistemas y aplicaciones se basa en la probabilidad de que una vulnerabilidad sea explotada y el impacto si la confidencialidad, integridad o disponibilidad de los activos de información se vieran comprometidas. La probabilidad de que se aproveche una vulnerabilidad aumenta en relación directa con la accesibilidad del sistema o la aplicación desde otros sistemas.
El impacto sobre los activos de información se basa en la clasificación de la información del activo (ver Norma de Clasificación de Información). Se debe considerar el impacto (es decir, alto, moderado o bajo) si la confidencialidad, integridad o disponibilidad se ve comprometida y se debe utilizar la calificación de impacto individual más alta para la confidencialidad, integridad o disponibilidad dentro de la siguiente tabla.

| Tabla 2: CLASIFICACIÓN DE RIESGO | | | |
|---|---|---|---|
| **Impacto (Confidencialidad, Integridad, Disponibilidad)** | **Exposición** | | |
| | **Sistemas sin conectividad de red a los datos de producción.** | **Sistemas con conectividad de red a datos de producción (sin acceso a Internet)** | **Sistema que está disponible públicamente en Internet.** |
| **Alto** | **Medio** | **Alto** | **Alto** |
| **Medio** | **Bajo** | **Medio** | **Alto** |
| **Bajo** | **Bajo** | **Bajo** | **Medio** |

La frecuencia mínima de los escaneos depende de la clasificación de riesgo. Los sistemas sin una clasificación de riesgo deben escanearse como si tuvieran una clasificación de riesgo "Alto" hasta que sean calificados.

| TABLA 3: FRECUENCIA DE ESCANEOS | |
|---|---|
| **Calificación de riesgo** | **Frecuencia** |
| **Escaneos de infraestructura** | |
| Alto | Mensual |
| Medio | Trimestral |
| Bajo | Semi anualmente |
| **Escaneos de aplicaciones web** | |
| Alto | Trimestralmente o después de un cambio significativo |
| Medio | Semi anualmente |
| Bajo | Anualmente |

### 2.4 Remediación

Las vulnerabilidades descubiertas durante los análisis deben remediarse según la clasificación de riesgo (consulte Tabla 2) y la gravedad de la vulnerabilidad identificada por la herramienta de escaneo según la siguiente tabla.

| TABLA 4: PLAZOS DE REMEDIACIÓN | | | |
|---|---|---|---|
| **Calificación de riesgo (de Tabla 2)** | **Gravedad de la vulnerabilidad** | | |
| | **Bajo o por debajo** | **Por encima de bajo a por debajo de alto** | **Alto o superior** |
| **Alto** | A discreción del ISO/encargado | Plan de acción en 2 semanas, | Plan de acción en 1 semana, |

| | | | |
|---|---|---|---|
| | de seguridad designado | resuelto en 6 3 meses | resuelto en 1 mes |
| **Medio** | A discreción del ISO/ encargado de seguridad designado | Plan de Acción en 3 Semanas, Resuelto en 1 6. Meses año | Plan de acción en 2 semanas, resuelto en 6 3 meses meses |
| **Bajo** | A discreción del ISO/ encargado de seguridad designado | A discreción del ISO/ encargado de seguridad designado | Plan de Acción en 3 Semanas, Resuelto en 1 6 meses año |

El encargado de seguridad designado/ISO puede revisar las vulnerabilidades para ajustar la clasificación de gravedad si es necesario. Se deben realizar pruebas para verificar que se haya completado la remediación.

Las personas que administran los análisis de vulnerabilidades deben notificar al ISO/encargado de seguridad designado dentro de **1 día hábil** después de la finalización del análisis para detectar nuevas vulnerabilidades y al menos una vez al mes para las vulnerabilidades no reparadas en sistemas o aplicaciones que se ejecutan en producción.

Los ISO/encargados de seguridad designados deben notificar a la gerencia sobre cualquier vulnerabilidad no remediada que no se haya abordado en los plazos prescritos en este estándar, de modo que la parte correspondiente acepte el riesgo.

## 3.0 Cumplimiento

Los empleados que incumplan esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y/o administrativas si correspondieren. Los no empleados, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

## 4.0 Definiciones de términos clave

| **Término** | Definición |
|---|---|
| **lite** | Hace referencia a una implementación leve o superficial. |

## 5.0 Historial de revisiones

| **Fecha** | **Descripción de Cambio** |
|---|---|
| 29/07/24 | Revisión de documento, agregado de definición de términos clave. |

## 6.0 Documentos relacionados

Estándar de Gestión de Parches.

# Capítulo 18

# Estándar de TI: Políticas de Mantenimiento

### 1.0 OBJETIVO

Garantizar que los recursos de tecnología de la información (TI) se mantengan de conformidad con las políticas, estándares y procedimientos de seguridad de TI.

### 2.0 POLÍTICA

Esta política es aplicable a todos los departamentos y usuarios de recursos y activos de TI.

1. MANTENIMIENTO CONTROLADO
   El Departamento de TI deberá:

   a. Programar, realizar, documentar y revisar registros de mantenimiento y reparaciones de componentes del sistema de información de acuerdo con las especificaciones y/o requisitos del fabricante o proveedor realizados por entidades de TI locales y/o subcontratadas.

   b. Aprobar y monitorear todas las actividades de mantenimiento, ya sea que se realicen en el sitio o de forma remota y si el equipo recibe servicio en el sitio o se traslada a otra ubicación.

   c. Exigir que los propietarios del sistema aprueben explícitamente la eliminación del sistema de información o de los componentes del sistema de las instalaciones para mantenimiento o reparación fuera del sitio.

   d. Desinfectar el equipo para eliminar toda la información de los medios asociados antes de retirarlo de las instalaciones de la Repartición para mantenimiento o reparaciones fuera del sitio.

   e. Verificar todos los controles de seguridad potencialmente afectados para chequear que sigan funcionando correctamente después de las acciones de mantenimiento o reparación.

   f. Incluir en los registros de mantenimiento la información relacionada con el mantenimiento definida por el propietario del sistema y de TI.

   g. Para aquellos componentes que no están directamente asociados con el procesamiento de información, como escáneres, fotocopiadoras e impresoras, los registros de mantenimiento deben incluir la fecha y hora del mantenimiento, la entidad que realiza el mantenimiento, el mantenimiento realizado, los

componentes reemplazados o eliminados, incluidos los números de identificación/serie, según corresponda.

2. HERRAMIENTAS DE MANTENIMIENTO
   El Departamento de TI deberá:

   a. Asegurarse de que los propietarios del sistema y TI aprueben, controlen y supervisen las herramientas de mantenimiento del sistema de información.

   b. Inspeccionar las herramientas de mantenimiento que el personal afín lleva a una instalación para detectar modificaciones inadecuadas o no autorizadas.

   c. Verificar los medios que contienen programas de diagnóstico y prueba para detectar códigos maliciosos antes de utilizarlos en el sistema de información.

3. MANTENIMIENTO NO LOCAL
   El Departamento de TI deberá:

   a. Aprobar y monitorear las actividades de diagnóstico y mantenimiento no locales.

   b. Permitir el uso de herramientas de diagnóstico y mantenimiento no locales solo según la política y documentados en el plan de seguridad del sistema de información.

   c. Emplear autenticadores sólidos en el establecimiento de sesiones de diagnóstico y mantenimiento no locales.

   d. Mantener registros de actividades de diagnóstico y mantenimiento no locales.

   e. Finalizar las conexiones de red y de sesión cuando se complete el mantenimiento no local.

   f. Documentar en el plan de seguridad del sistema de información, las políticas y procedimientos para el establecimiento y uso de conexiones no locales de mantenimiento y diagnóstico.

4. PERSONAL DE MANTENIMIENTO
   El Departamento de TI deberá:

   a. Establecer un proceso para la autorización del personal de mantenimiento y conservar una lista de organizaciones o personal autorizado.

   b. Asegurar que el personal no acompañado que realiza el mantenimiento del sistema de información tenga las autorizaciones de acceso requeridas.

c. Designar personal con las autorizaciones de acceso requeridas y competencia técnica para supervisar las actividades de mantenimiento del personal que no posee las autorizaciones de acceso requeridas.

5. MANTENIMIENTO OPORTUNO
   El Departamento de TI deberá:

   a. Obtener soporte de mantenimiento y/o repuestos para sistemas de información según lo acordado dentro del acuerdo de nivel de servicio entre TI y el propietario del sistema.

## 3.0 CUMPLIMIENTO

Los empleados que incumplan esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y/o administrativas si correspondieren. Los no empleados, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

## 4.0 EXCEPCIONES DE POLÍTICA

Las solicitudes de excepciones a esta política serán revisadas por el Director de Ciberseguridad (DC) y la Secretaría de Innovación Pública (SIP) y/o Encargado de Seguridad de la Información. Los departamentos que soliciten excepciones deberán proporcionar dichas solicitudes al DC /SIP. La solicitud debe indicar específicamente el alcance de la excepción junto con la justificación para otorgar la excepción, el posible impacto o riesgo asociado al otorgar la excepción, las medidas de mitigación de riesgos que debe tomar el Departamento de TI, iniciativas, acciones y un cronograma para lograrlo, el nivel mínimo de cumplimiento de las políticas aquí establecidas. El DC/SIP revisará dichas solicitudes; consultar con el departamento solicitante.

## 5.0 HISTORIAL DE REVISIONES

| Fecha | Descripción de Cambio | Autores |
|---|---|---|
| 18/07/24 | Visado de documento | Pablo Zalazar, Alejandro Castro |
| 30/07/24 | Revisión de Documento, corrección de errores, ajuste de formato. | Alejandro Castro |

## 6.0 REFERENCIA

Publicaciones especiales (SP) del Instituto Nacional de Estándares y Tecnología (NIST): NIST SP 800-53: mantenimiento del sistema (MA), NIST SP 800-12, NIST SP 800-63, NIST

SP 800-88, NIST SP 800-100; Estándares federales de procesamiento de información (FIPS) 140-2, FIPS 197, FIPS 201

# Capítulo 19

# Estándar de TI: Política de Protección de Medios

### 1.0 OBJETIVO

Garantizar que la tecnología de la información (TI) controle el acceso y elimine los recursos multimedia de conformidad con las políticas, estándares y procedimientos de seguridad de TI.

### 2.0 POLÍTICA

Esta política es aplicable a todos los departamentos y usuarios de recursos y activos de TI.

1. ACCESO A LOS MEDIOS:
   TI, a través de la dirección de las reparticiones, deberá:

   a. Restringir el acceso a tipos definidos de medios digitales y/o no digitales a personal identificado.

   b. Marcar los medios del sistema de información indicando las limitaciones de distribución, las advertencias de manejo y las marcas de seguridad aplicables de los medios de información digitales y no digitales.

2. ALMACÉN DE DATOS
   El Departamento de TI deberá:

   a. Especificar el personal para controlar físicamente y almacenar de forma segura los medios dentro de áreas controladas definidas.

   b. Proteger los medios del sistema de información hasta que los medios sean destruidos o desinfectados utilizando equipos, técnicas y procedimientos aprobados.

3. TRANSPORTE DE MEDIOS
   El Departamento de TI deberá:

   a. Proteger y controlar los medios durante el transporte fuera de áreas controladas.

   b. Mantener la trazabilidad de los medios del sistema de información durante el transporte fuera de las áreas controladas.

   c. Documentar las actividades asociadas al transporte de soportes de sistemas de información.

   d. Restringir las actividades asociadas al transporte de soportes de sistemas de información al personal autorizado.

4. SANITIZACIÓN DE MEDIOS
   El Departamento de TI deberá:

   a. Desinfectar antes de desecharlo, liberarlo fuera del control de la organización o liberarlo para su reutilización utilizando un estándar especificado por la Repartición de acuerdo con las normas y políticas nacionales, provinciales y organizacionales aplicables.

   b. Emplear mecanismos de sanitización con la solidez e integridad acorde a la categoría o clasificación de seguridad de la información.

5. USO DE MEDIOS
   El Departamento de TI deberá:

   Prohibir el uso de cualquier tipo de medio del sistema de información definidos por la Repartición en los equipos propios, utilizando medidas de seguridad no aprobadas.

## 3.0 CUMPLIMIENTO

Los empleados que incumplan esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y/o administrativas si correspondieren. Los no empleados, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

## 4.0 EXCEPCIONES DE POLÍTICA

Las solicitudes de excepciones a esta política serán revisadas por el Director de Ciberseguridad (DC) y la Secretaría de Innovación Pública (SIP) y/o Encargado de Seguridad de la Información. Los departamentos que soliciten excepciones deberán proporcionar dichas solicitudes al DC/SIP. La solicitud debe indicar específicamente el

alcance de la excepción junto con la justificación para otorgar la excepción, el posible impacto o riesgo asociado al otorgar la excepción, las medidas de mitigación de riesgos que debe tomar el Departamento de TI, iniciativas, acciones y un cronograma para lograrlo, el nivel mínimo de cumplimiento de las políticas aquí establecidas. El DC/SIP revisará dichas solicitudes; consultar con el departamento solicitante.

## 5.0 HISTORIAL DE REVISIONES

| Fecha | Descripción de Cambio | Autores |
|---|---|---|
| 19/07/24 | Visado de documento. | Pablo Zalazar, Alejandro Castro |
| 31/07/24 | Revisión de Documento, corrección de errores, ajuste de formato. | Alejandro Castro |

## 6.0 REFERENCIA

Publicaciones especiales (SP) del Instituto Nacional de Estándares y Tecnología (NIST): NIST SP 800-53: protección de medios (MP), NIST SP 800-12, NIST SP 800-56, NIST SP 800-57, NIST SP 800-60, NIST SP 800-88, NIST SP 800-100, NIST SP 800-111; NIST Estándares federales de procesamiento de información (FIPS)199.

# Capítulo 20

# Política de Autorización y Evaluación de Seguridad

## 1.0 OBJETIVO

Las Tecnologías de la Información (TI) y las diversas unidades gubernamentales (propietarios de la información) garantizarán los controles de seguridad en los sistemas de información y los entornos en los que operan esos sistemas, como parte de las autorizaciones de seguridad iniciales y continuas, las evaluaciones anuales, el monitoreo continuo y las actividades del ciclo de vida del desarrollo del sistema.

## 2.0 POLÍTICA

Esta política es aplicable a todos los departamentos y usuarios de recursos y activos de TI. Cada dependencia que mantiene o recopila activos de información debe cumplir con esta política.

1. POLÍTICA Y PROCEDIMIENTOS DE EVALUACIÓN Y AUTORIZACIÓN DE SEGURIDAD
   La Repartición deberá:

   a. Desarrollar, documentar y difundir a personal o roles definidos por la Repartición:

      i. Una política de evaluación y autorización de seguridad que aborda el propósito, el alcance, las funciones, las responsabilidades, el compromiso de la administración, la coordinación entre las entidades organizacionales y el cumplimiento.

      ii. Procedimientos para facilitar la implementación de la política de autorización y evaluación de seguridad y los controles de autorización y evaluación de seguridad asociados.

   b. Revisar y actualizar la política y los procedimientos actuales de evaluación y autorización de seguridad en una frecuencia anual.

2. EVALUACIONES DE SEGURIDAD
   La Repartición deberá:

a. Desarrollar un plan de evaluación de seguridad que describa el alcance de la evaluación, incluyendo:

    i. Controles de seguridad y mejoras de control en evaluación.

    ii. Procedimientos de evaluación que se utilizarán para determinar la eficacia del control de seguridad.

    iii. Entorno de evaluación, equipo de evaluación y roles y responsabilidades de evaluación.

b. Evaluar los controles de seguridad en el sistema de información y su entorno de operación en una frecuencia definida por la Repartición determinar en qué medida los controles se implementan correctamente, funcionan según lo previsto y producen el resultado deseado con respecto al cumplimiento de los requisitos de seguridad establecidos.

c. Producir un informe de evaluación de seguridad que documente los resultados de la evaluación.

d. Proporcionar los resultados de la evaluación del control de seguridad a individuos o roles definidos por la Repartición.

3. INTERCONEXIONES DEL SISTEMA
El Departamento de TI deberá:

a. Autorizar conexiones entre los sistemas de información mediante el uso de Acuerdos de Seguridad de Interconexión.

b. Documentar, para cada interconexión, las características de la interfaz, los requisitos de seguridad y la naturaleza de la información comunicada.

c. Revisar y actualizar Acuerdos de Seguridad de Interconexión en una frecuencia semestral.

d. Emplear una política de permitir todo, denegar por excepción, denegar todo, permitir por excepción, para permitir sistemas de información definidos por la Repartición para conectarse a sistemas de información externos.

4. PLAN DE ACCIÓN E HITOS
   La Repartición deberá:

   a. Desarrollar un plan de acción e hitos para el sistema de información para documentar las acciones correctivas planificadas para corregir las debilidades o deficiencias observadas durante la evaluación de los controles de seguridad y para reducir o eliminar las vulnerabilidades conocidas en el sistema.

   b. Actualizar el plan de acción y los hitos existentes en una frecuencia definida por la Repartición basado en los hallazgos de las evaluaciones de los controles de seguridad, los análisis de impacto de la seguridad y las actividades de monitoreo continuo.

5. AUTORIZACIÓN DE SEGURIDAD
   La Repartición deberá:

   a. Designar a un funcionario, jefe de área o de departamento como autorizador del sistema de información.

   b. Asegurar que el funcionario designado autorice el procesamiento del sistema de información antes de iniciar las operaciones.

   c. Actualizar la autorización de seguridad en una frecuencia definida por la Repartición.

6. MONITOREO CONTINUO
   El Departamento de TI deberá:

   a. Desarrollar una estrategia de monitoreo continuo e implementar un programa que incluya:

      i. Establecimiento de métricas definidas por la Repartición para ser monitoreado.

      ii. Establecimiento de frecuencias definidas por la Repartición para el seguimiento y frecuencias definidas por la Repartición para evaluaciones que respalden dicho seguimiento.

      iii. Evaluaciones continuas del control de seguridad de acuerdo con la estrategia organizacional de seguimiento continuo.

      iv. Monitoreo continuo del estado de seguridad de las métricas definidas por la organización de acuerdo con la estrategia de monitoreo continuo de la organización.

v. Correlación y análisis de información relacionada con la seguridad generada por evaluaciones y monitoreo.

vi. Acciones de respuesta para atender resultados del análisis de información relacionada con la seguridad.

vii. Informar del estado de seguridad de la organización y del sistema de información a personal o roles definidos por la Repartición en una frecuencia definida por la Repartición.

7. CONEXIONES DEL SISTEMA INTERNO
   El Departamento de TI deberá:

   a. Autorizar conexiones internas de componentes o clases de componentes del sistema de información definidos por la Repartición al sistema de información.

   b. Documentar, para cada conexión interna, las características de la interfaz, los requisitos de seguridad y la naturaleza de la información comunicada.

## 3.0 CUMPLIMIENTO

Los empleados que incumplan esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y/o administrativas si correspondieren. Los no empleados, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

## 4.0 EXCEPCIONES DE POLÍTICA

Las solicitudes de excepciones a esta política serán revisadas por el Director de Ciberseguridad (DC) y la Secretaría de Innovación Pública (SIP) y/o Encargado de Seguridad de la Información. Los departamentos que soliciten excepciones deberán proporcionar dichas solicitudes al DC/SIP. La solicitud debe indicar específicamente el alcance de la excepción junto con la justificación para otorgar la excepción, el posible impacto o riesgo asociado al otorgar la excepción, las medidas de mitigación de riesgos que debe tomar el Departamento de TI, iniciativas, acciones y un cronograma para lograrlo, el nivel mínimo de cumplimiento de las políticas aquí establecidas. El DC/SIP revisará dichas solicitudes; consultar con el departamento solicitante.

## 5.0 HISTORIAL DE REVISIONES

| Fecha | Descripción de Cambio | Autores |
|---|---|---|
| 19/07/24 | Visado de documento. | Pablo Zalazar, Alejandro Castro |

| | | |
|---|---|---|
| 31/07/24 | Revisión de Documento, corrección de errores, ajuste de formato. | Alejandro Castro |

## 6.0 REFERENCIA

Publicaciones especiales (SP) del Instituto Nacional de Estándares y Tecnología (NIST): NIST SP 800-53a: Evaluación y autorización de seguridad (CA), NIST SP 800-12, NIST SP 800-37, NIST SP 800-39, NIST SP 800-47, NIST SP 800-100, NIST SP 800-115, NIST SP 800-137; Estándares federales de procesamiento de información (FIPS) 199 del NIST

# Capítulo 21

# Política de Auditoria y Rendición de Cuentas

### 1.0 OBJETIVO

Garantizar que los recursos y sistemas de información de tecnología de la información (TI) se establezcan con controles de seguridad efectivos y mejoras de control que reflejen las leyes, órdenes ejecutivas, directivas, regulaciones, políticas, estándares y directrices Nacionales y Provinciales aplicables.

### 2.0 POLÍTICA

Esta política es aplicable a todos los departamentos y usuarios de recursos y activos de TI.

1. EVENTOS DE AUDITORÍA
   Los propietarios de los sistemas de información, en cooperación con las auditorías y las TI, deberán:

a. Determinar que el sistema de información es capaz de auditar los siguientes eventos: inicio de sesión (exitoso, fallido, o cambio de contraseña) con respecto a archivos, creación, eliminación y tipo de red utilizada, configuración de GPOs, instalación de softwares, intentos de accesos por softwares o hardwares. Tiempo de actividad.
    a. El sistema de información deberá registrar los siguientes, entre otros eventos definidos por la Repartición:
        i. **Acceso al sistema:** Inicio de sesión (exitoso, fallido, cambio de contraseña) Intentos de acceso no autorizados (por software o hardware)
        ii. **Gestión de archivos:** Creación, modificación y eliminación de archivos
        iii. **Configuración del sistema:** Cambios en la configuración de GPOs, Instalación y desinstalación de software
    b. Uso de la red:
        i. Tipo de red utilizada en cada conexión.

b. Coordinar la función de auditoría de seguridad con otras Reparticiones que requieran auditoría, y fijar objetivos comunes. Con ese objetivo, deberán definirse procesos de recopilación, análisis y respuestas, así como frecuencias de coordinación y resguardo de los resultados.

c. Proporcionar una justificación de por qué los eventos auditables se consideran adecuados para respaldar las investigaciones posteriores a los incidentes de seguridad.

d. Determinar que dentro del sistema de información se deben auditar los siguientes eventos: inicio de sesión (exitoso, fallido, o cambio de contraseña) con respecto a archivos, creación, eliminación y tipo de red utilizada, configuración de GPOs, instalación de softwares, intentos de accesos por softwares o hardwares.

2. RESEÑAS Y ACTUALIZACIONES

    a. Se deberá revisar y actualizar los eventos auditados en una frecuencia definida por la Repartición

3. CONTENIDO DE LOS REGISTROS DE AUDITORÍA

    a. El sistema de información generará registros de auditoría, éstos contendrán información sobre: qué tipo de evento ocurrió, cuándo ocurrió, dónde ocurrió, la fuente del evento, el resultado del evento y la identidad de cualquier individuo o sujeto asociado con el evento.

4. INFORMACIÓN ADICIONAL DE AUDITORÍA

    a. El sistema de información generará registros de auditoría que contengan información adicional, quedando en la Repartición la definición de los datos de información adicional y más detallada, siendo optativo de acuerdo a los recursos humanos y tecnológicos disponibles.

5. CAPACIDAD DE ALMACENAMIENTO DE AUDITORÍA

    a. El propietario de la información deberá garantizar que la capacidad de almacenamiento de registros de auditoría se asigne de acuerdo con adonde se almacena y como se buscan los registros.

6. TRANSFERENCIA A ALMACENAMIENTO ALTERNO

    a. El sistema de información descargará los registros de auditoría en una frecuencia definida por la Repartición, en un sistema o medio diferente al sistema que se está auditando.

7. RESPUESTA A FALLAS EN EL PROCESAMIENTO DE AUDITORÍA
   El sistema de información deberá:

    a. Alertar al superior inmediato que ha solicitado la auditoria, personal o roles definidos por la Repartición en caso de una falla en el proceso de auditoría.

    b. Realizar acciones adicionales. La Repartición definirá las acciones que se deben tomar al procesar la falla; y (por ejemplo, cerrar el sistema de información, sobrescribir los registros de auditoría más antiguos, dejar de generar registros de auditoría).

8. CAPACIDAD DE ALMACENAMIENTO DE AUDITORÍA

    a. El sistema de información proporcionará un aviso al encargado de seguridad de la información o IT asignado, personal, roles y/o ubicaciones definidos por la Repartición dentro de una frecuencia a definir por la Repartición (se sugiere en un rango de tiempo máximo de 24 horas) cuando se alcanza el volumen de almacenamiento de registros de auditoría asignado, en un porcentaje definido por la Repartición (se sugiere no superior al 90%) de la capacidad máxima de almacenamiento de registros de auditoría del repositorio.

9. ALERTAS EN TIEMPO REAL

    a. El sistema de información proporcionará una alerta al superior jerárquico, personal, roles y/o agentes definidos por la Repartición cuando ocurran los siguientes eventos de falla de auditoría:

        i. Eventos de falla de auditoría definidos por la Repartición que requieren alertas en tiempo real.

    Ante la detección de eventos de falla en el proceso de auditoría, configurados previamente por la Repartición, el sistema generará alertas inmediatas. Estas alertas serán enviadas a los usuarios, roles o agentes especificados, a través de los canales de comunicación definidos (correo electrónico, SMS, notificaciones push, etc.). Los eventos de falla a monitorear podrán incluir, entre otros, la pérdida de datos de auditoría, la incapacidad de generar nuevos registros o la detección de anomalías en los datos.

10. UMBRALES DE VOLUMEN DE TRÁFICO CONFIGURABLES

    El sistema de información aplicará umbrales de volumen de tráfico de comunicaciones de red configurables que reflejen los límites de la capacidad de auditoría y rechazará o retrasará el tráfico de red por encima de esos umbrales.
    Para garantizar la eficiencia de la auditoría, el sistema establecerá límites máximos de tráfico de red. Cualquier comunicación que exceda estos umbrales será bloqueada o su procesamiento será pospuesto hasta que la situación de la red lo permita.

11. APAGADO EN CASO DE FALLA

    El sistema de información invocará un apagado completo del sistema; apagado parcial del sistema; modo operativo degradado con funcionalidad limitada de misión disponible en el caso de fallos de auditoría definidos por la Repartición, a menos que exista una capacidad de auditoría alternativa.
    Para proteger la integridad de los datos y garantizar la seguridad del sistema, ante la detección de un fallo de auditoría, se implementará una de las siguientes

acciones: apagado total, apagado parcial o transición a un modo operativo restringido. Estas medidas se activarán a menos que exista una solución de auditoría alternativa que permita continuar las operaciones.

12. REVISIÓN, ANÁLISIS E INFORMES DE AUDITORÍA

El propietario del sistema de información deberá:

a. Revisar y analizar registros de auditoría del sistema de información. En una frecuencia definida por la Repartición para indicaciones de actividad inapropiada o inusual que se haya definido por la Repartición.

b. Informar los hallazgos a personal o roles definidos por la Repartición, en caso de contar con órgano auditor, debe ser a esta entidad.

13. INTEGRACIÓN DE PROCESOS

Los propietarios del sistema de información deberán garantizar que se empleen mecanismos automatizados para integrar los procesos de revisión, análisis y presentación de informes de auditoría para respaldar los procesos organizacionales de investigación y respuesta a actividades sospechosas.

14. REPOSITORIOS DE AUDITORÍA

El propietario del sistema de información deberá garantizar el análisis y la correlación de los registros de auditoría en diferentes repositorios para obtener conocimiento de la situación. (documentación, evidencia de auditorías, papeles de trabajo, informe final y presentación).

15. REDUCCIÓN DE AUDITORÍAS Y GENERACIÓN DE INFORMES

a. El sistema de información deberá proporcionar una capacidad de reducción de auditorías y generación de informes que:

   i. Admita requisitos de revisión, análisis e informes de auditoría bajo demanda y a posteriori.

   ii. No altere el contenido original ni el orden temporal de los registros de auditoría.

16. PROCESAMIENTO AUTOMÁTICO

El sistema de información deberá contar con la capacidad de procesar registros de auditoría para eventos de interés, basados en campos o datos de auditoría definidos por la Repartición dentro de los registros de auditoría. Permitiendo a la Repartición definir los criterios de filtrado según sus necesidades

17. MARCAS DE TIEMPO
    El sistema de información deberá:

    a. Utilizar relojes internos del sistema para generar marcas de tiempo para los registros de auditoría.

    b. Registrar marcas de tiempo para registros de auditoría que se pueden asignar a la hora universal coordinada (UTC) o a la hora media de Greenwich (GMT) y cumple granularidad definida por la Repartición de la medición del tiempo, en situaciones de cambios de horario.

18. SINCRONIZACIÓN CON FUENTE DE TIEMPO AUTORIZADA
    El sistema de información deberá:

    a. Comparar los relojes del sistema de información interno en una frecuencia definida por la Repartición, con el servicio oficial de horario NTP, sugiriéndose que sea una entidad nacional de servicio NTP. actualmente el Servicio Público Nacional de la Hora Oficial (Decreto del Poder Ejecutivo Nacional Nº 1792/83).

    b. Sincronizar los relojes internos del sistema con servicio horario autorizado cuando la diferencia horaria sea mayor que un período de tiempo definido por la Repartición.

19. PROTECCIÓN DE LA INFORMACIÓN DE AUDITORÍA

    a. El sistema de información deberá proteger la información de auditoría y las herramientas de auditoría contra el acceso, modificación y eliminación no autorizados.
       El sistema implementará medidas de seguridad para garantizar la confidencialidad, integridad y disponibilidad de la información y las herramientas de auditoría, protegiéndolas contra cualquier acceso, modificación o eliminación no autorizada.

20. ACCESO POR SUBCONJUNTO DE USUARIOS CON PRIVILEGIO DE AUTORIZACIÓN

    a. La Repartición debe autorizar el acceso a la gestión de la funcionalidad de auditoría solo a un subconjunto de usuarios con privilegios de acceso definido por Repartición.

21. RETENCIÓN DE REGISTROS DE AUDITORÍA

    a. Los propietarios del sistema de información conservarán registros de auditoría durante el período de tiempo definido por la Repartición consistente con la política de retención de registros para brindar soporte a investigaciones de incidentes de seguridad y cumplir con los requisitos regulatorios de Plazos Mínimos de

Conservación y Guarda de Actuaciones Administrativas actualmente RESOL-2019-94-APN-SECMA#JGM.
Los propietarios del sistema garantizarán la conservación de los registros de auditoría durante el tiempo definido por la Repartición. Esta medida tiene como objetivo respaldar futuras investigaciones de incidentes de seguridad y asegurar el cumplimiento de las normativas legales y gubernamentales en materia de retención de datos.

22. CAPACIDAD DE RECUPERACIÓN A LARGO PLAZO

a. Los propietarios del sistema de información deberán emplear medidas definidas por la Repartición para garantizar que se puedan recuperar los registros de auditoría a largo plazo generados por el sistema de información.

23. GENERACIÓN DE AUDITORÍA
El sistema de información deberá:

a. Proporcionar capacidad de generación de registros de auditoría para los eventos auditables según lo definido en los componentes del sistema de información definidos por la Repartición.

b. Permitir al personal o los roles definidos por la Repartición (usuarios definidos en el punto 20) seleccionar qué eventos deben ser auditados por componentes específicos del sistema de información.

c. Generar registros de auditoría de los eventos con el contenido definido en componentes del sistema de información definidos por la Repartición.

24. REGISTRO DE AUDITORÍA CORRELACIONADO CON EL TIEMPO

a. El sistema de información deberá cumplir con los registros de auditoría de los componentes, definidos por la Repartición, en un registro de auditoría de todo el sistema (lógica o física) que está correlacionado en el tiempo dentro de un nivel de tolerancia, definido por la Repartición, para la relación entre marcas de tiempo de registros individuales en el registro de auditoría.
El sistema integrará los registros de auditoría de sus diversos componentes en un único repositorio, garantizando que los eventos estén ordenados cronológicamente de manera precisa y coherente, conforme a los requisitos de tolerancia temporal definidos por la Repartición.

25. FORMATOS ESTANDARIZADOS

a. Correlacionado con el formato, el sistema de información deberá producir un registro centralizado de auditoría (lógica o física) para todo el sistema compuesto de registros de auditoría en un formato estandarizado. Deberá integrar los

registros de auditoría de todos sus componentes para facilitar su análisis y consulta.

26. CAMBIOS POR PERSONAS AUTORIZADAS

    a. El sistema de información deberá proporcionar la capacidad a individuos o roles previamente definidos, para cambiar la auditoría que se realizará en componentes del sistema de información ya definidos, basados en criterios de eventos seleccionables dentro de umbrales de tiempo definidos por la Repartición.

## 3.0 CUMPLIMIENTO

Los empleados que incumplan esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y/o administrativas si correspondieren. Los terceros ajenos a la repartición, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

## 4.0 EXCEPCIONES DE POLÍTICA

Las solicitudes de excepciones a esta política serán revisadas por el Director de Ciberseguridad (DC) y Secretaría de Innovación Pública (SIP) y/o Encargado de Seguridad de la Información. Los departamentos que soliciten excepciones deberán proporcionar dichas solicitudes al DC/SIP. La solicitud debe indicar específicamente el alcance de la excepción junto con la justificación para otorgar la excepción, el posible impacto o riesgo asociado al otorgar la excepción, las medidas de mitigación de riesgos que debe tomar el Departamento de TI, iniciativas, acciones y un cronograma para lograrlo, el nivel mínimo de cumplimiento de las políticas aquí establecidas. El DC/SIP revisará dichas solicitudes; consultar con el departamento solicitante.

## 5.0 DEPARTAMENTO RESPONSABLE

Oficina principal de información y propietarios de sistemas de información

## 6.0 HISTORIAL DE REVISIONES

| Fecha | Descripción de Cambio | Participantes |
|---|---|---|
| 01/08/2024 | Revisión inicial | Alejandro Castro, Pablo Zalazar |
| 26/08/2024 | Visado, y corrección de errores | Alejandro Castro, Paula D'Agostino |

## 7.0 REFERENCIA

Publicaciones especiales (SP) del Instituto Nacional de Estándares y Tecnología (NIST): NIST SP 800-53a - Auditoría y Responsabilidad (AU), NIST SP 800-12, NIST SP 800-92, NIST SP 800-100

# Capítulo 22

# Desinfección/Eliminación Segura

## 1.0 Propósito y Beneficios

Los sistemas de información capturan, procesan y almacenan información utilizando una amplia variedad de medios, incluido el papel. Esta información no sólo se encuentra en el medio de almacenamiento previsto, sino también en los dispositivos utilizados para crear, procesar o transmitir esta información. Estos medios pueden requerir una disposición especial para mitigar el riesgo de divulgación no autorizada de información y garantizar su confidencialidad.

## 2.0 Declaración de información

De acuerdo con la Política de Seguridad de la Información, la información debe ser adecuadamente gestionada desde su creación, pasando por el uso autorizado, hasta su adecuada disposición.

La Repartición debe garantizar que los usuarios y custodios de la información sean conscientes de su sensibilidad y de los requisitos básicos para la desinfección de los medios y su eliminación segura.

La Repartición debe garantizar que todos los agentes administrativos, profesionales y técnicos, incluidos los administradores, conozcan el proceso de desinfección de los medios y eliminación segura para establecer la responsabilidad adecuada de todos los datos.

La Repartición debe garantizar que el material confidencial sea destruido únicamente por personal autorizado y capacitado, ya sea interno o contratado, utilizando los métodos descritos en esta norma.

La Repartición podrá utilizar proveedores de servicios con fines de destrucción siempre que la información permanezca segura hasta que se complete la destrucción. Los proveedores de servicios deben seguir este estándar. La entidad debe asegurarse de que existan acuerdos contractuales o de mantenimiento que sean suficientes para proteger la confidencialidad de los medios y la información del sistema de manera acorde con los estándares de clasificación de la información.

**Métodos de desinfección de medios**

La siguiente tabla muestra los tres tipos de métodos de desinfección y el impacto de cada método.

| Método de desinfección | Uso apropiado | Descripción |
|---|---|---|
| Borrar | Si los medios serán reutilizados y no saldrán del control de la entidad. | Protege la confidencialidad de la información contra un ataque reemplazando los datos escritos con datos aleatorios. La limpieza no debe permitir que las utilidades de recuperación de datos, discos o archivos recuperen información. |
| Purgar | Si los medios serán reutilizados y saldrán del control de la entidad. | Protege la confidencialidad de la información contra un ataque mediante desmagnetización o borrado seguro. |
| Destrucción física | Si los medios no se reutilizarán en absoluto. | La intención es destruir completamente los medios. |

## Proceso de decisión de desinfección

El proceso de decisión se basa en la confidencialidad de la información, no en el tipo de medio. Las Reparticiones eligen el tipo de sanitización a utilizar, y el tipo de sanitización es aprobado por el propietario de la Información. La técnica utilizada puede variar según el tipo de medio y la tecnología disponible para el custodio, siempre y cuando se cumplan los requisitos del tipo de sanitización. Las técnicas de desinfección recomendadas para tipos específicos de medios se describen en el Apéndice A de NIST 800-88, Rev. 1, Pautas para la desinfección de medios, Recomendaciones mínimas de desinfección.

La eliminación sin desinfección debe considerarse solo si la divulgación de información no tendría impacto en la misión gubernamental, no resultaría en daños a los activos del Gobierno de Jujuy y no resultaría en pérdidas financieras o daños a ningún individuo.

La categorización de seguridad de la información, junto con los factores ambientales internos, deberían impulsar las decisiones sobre cómo tratar con los medios. La clave es pensar primero en términos de confidencialidad de la información y luego aplicar consideraciones basadas en el tipo de medio.

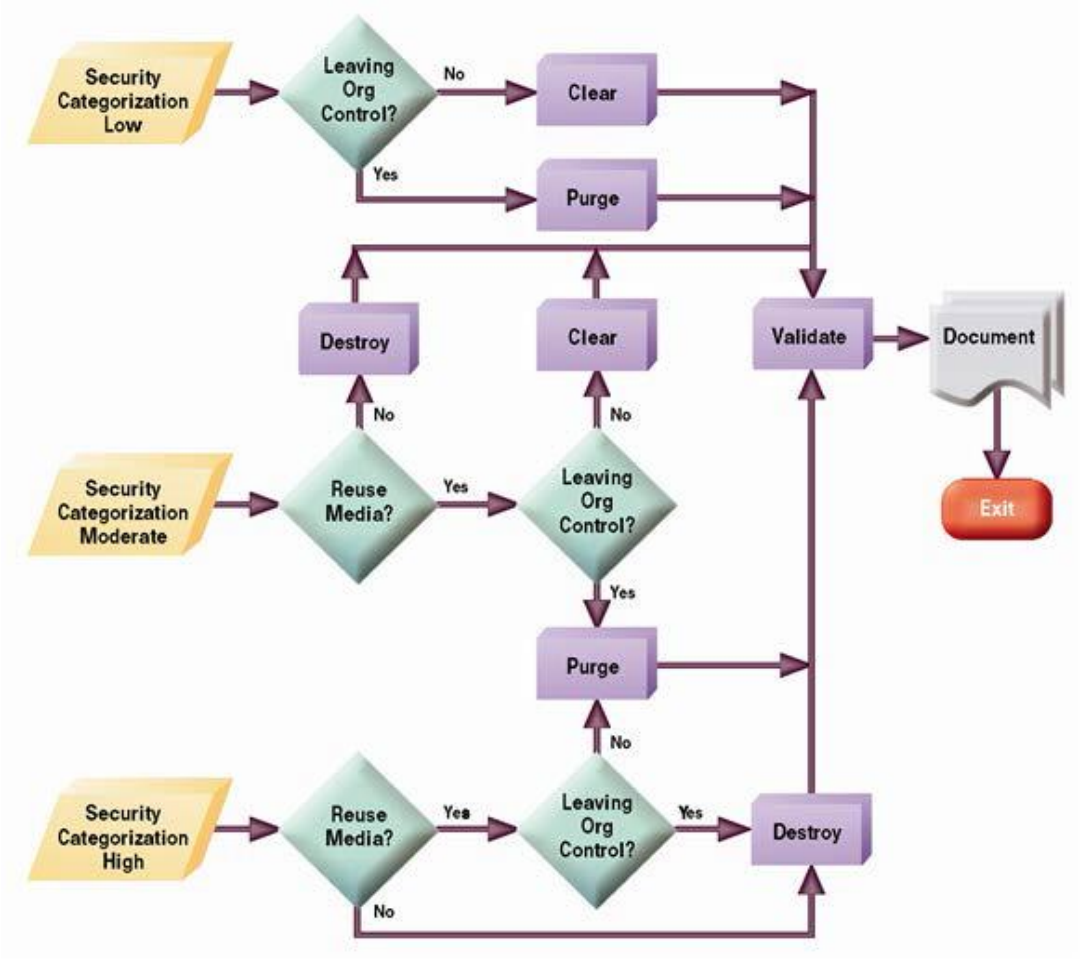


Figura 4.1- Flujo de decisiones de desinfección y disposición
(de NIST 800-88, Rev. 1, Directrices para la desinfección de medios)

Se debe comprender el costo versus el beneficio de un proceso de desinfección antes de tomar una decisión final. Las Reparticiones siempre pueden aumentar el nivel de saneamiento aplicado si ello es razonable y así lo indica una evaluación del riesgo existente. Por ejemplo, aunque Clear o Purge puede ser la solución recomendada, puede ser más rentable (teniendo en cuenta la capacitación, el seguimiento y la validación, etc.) destruir los medios en lugar de utilizar una de las otras opciones. Las Reparticiones no podrán disminuir el nivel de sanitización requerido.

**Control de medios**

Un factor que influye en una decisión de desinfección es quién tiene control y acceso a los medios. Este aspecto debe ser considerado cuando los medios abandonan el control gubernamental. El control de los medios puede transferirse cuando los medios se devuelven de un contrato de locación o se donan o revenden para ser reutilizados fuera de la gobernación. Los siguientes son ejemplos de control de medios:

Bajo control:

- Los medios que se entregan para mantenimiento todavía se consideran bajo el control de la Repartición si existen acuerdos contractuales y el proveedor de mantenimiento prevé específicamente la confidencialidad de la información.

- El mantenimiento realizado en el sitio de una Repartición, bajo la supervisión de la Repartición, por un proveedor de mantenimiento también se considera bajo el control de la Repartición.

No bajo control de la Repartición:

- Los medios que se intercambian por garantía, reembolso de costos u otros fines y donde los medios específicos no serán devueltos a la Repartición se consideran fuera del control de la Repartición.

**Reutilización de medios**

Las Reparticiones deben considerar el costo versus el beneficio de la reutilización. Puede ser más rentable (teniendo en cuenta la capacitación, el seguimiento y la validación, etc.) destruir los medios en lugar de utilizar una de las otras opciones.

**Limpiar / Purgar / Destruir**

| Método | Descripción |
|---|---|
| Borrar | Un método para desinfectar los medios es utilizar productos de software o hardware para sobrescribir el espacio de almacenamiento direccionable por el usuario en los medios con datos no confidenciales, utilizando los comandos estándar de lectura y escritura para el dispositivo. Este proceso puede incluir sobrescribir no sólo la ubicación de almacenamiento lógico de un archivo (por ejemplo, tabla de asignación de archivos), sino que también debe incluir todas las ubicaciones direccionables por el usuario. El objetivo de seguridad del proceso de sobrescritura es reemplazar los datos de destino con datos no confidenciales. La sobrescritura no se puede utilizar para medios dañados o que no se pueden reescribir y es posible que no aborde todas las áreas del dispositivo donde se pueden conservar datos confidenciales. El tipo y tamaño del medio también pueden influir en si la sobrescritura es un método de desinfección adecuado. Por ejemplo, los dispositivos de almacenamiento basados en memoria flash pueden contener celdas de repuesto y realizar una nivelación de desgaste, lo que hace que sea inviable para un usuario desinfecte todos los datos anteriores usando este enfoque porque es posible que el dispositivo no admita abordar directamente todas las áreas donde se han almacenado datos confidenciales usando el Interfaz nativa de lectura y escritura.<br>La operación Borrar puede variar contextualmente para medios que no sean dispositivos de almacenamiento dedicados, donde el dispositivo (como un teléfono celular básico o un equipo de oficina) solo brinde la capacidad de devolver el dispositivo al estado de fábrica (generalmente simplemente eliminando los punteros del archivo) y no admite directamente la capacidad de reescribir o aplicar técnicas específicas de medios a los contenidos de almacenamiento no volátiles. Cuando no se admite la reescritura, los restablecimientos del fabricante y los procedimientos que no incluyen la reescritura pueden ser la única opción para borrar el dispositivo y los medios asociados. Estos aún cumplen con la definición de Borrado siempre que la interfaz del dispositivo disponible para el usuario no facilite la recuperación de los datos borrados. |
| Purgar | Algunos métodos de purga (que varían según el medio y deben aplicarse teniendo en cuenta las consideraciones que se describen más adelante a lo largo de este documento) incluyen la sobrescritura, el borrado de bloques y el borrado criptográfico, mediante el uso de comandos de desinfección de dispositivos estandarizados y dedicados que aplican |

| | |
|---|---|
| | técnicas específicas de los medios para evitar la abstracción inherente a los comandos típicos de lectura y escritura.<br>Las técnicas destructivas también hacen que el dispositivo se purgue cuando se aplican eficazmente al tipo de medio apropiado, incluida la incineración, trituración, desintegración, desmagnetización y pulverización. El beneficio común de todos estos enfoques es la garantía de que no es posible recuperar los datos utilizando técnicas de laboratorio de última generación. Sin embargo, doblar, cortar y el uso de algunos procedimientos de emergencia (como usar un arma de fuego para perforar un dispositivo de almacenamiento) solo pueden dañar el medio, ya que algunas partes del medio pueden permanecer intactas y, por lo tanto, ser accesibles mediante técnicas de laboratorio avanzadas.<br>La desmagnetización hace que un dispositivo magnético heredado se purgue cuando la fuerza del desmagnetizador se adapta cuidadosamente a la coercitividad del medio. Puede ser difícil determinar la coercitividad basándose únicamente en la información proporcionada en la etiqueta. Por lo tanto, consulte al fabricante del dispositivo para obtener detalles sobre la coercitividad. Nunca se debe confiar únicamente en la desmagnetización para dispositivos de almacenamiento basados en memoria flash o para dispositivos de almacenamiento magnéticos que también contienen almacenamiento no volátil y no magnético. La desmagnetización inutiliza muchos tipos de dispositivos (y en esos casos, la desmagnetización también es una técnica de destrucción). |
| Destruir | Existen muchos tipos, técnicas y procedimientos diferentes para la destrucción de medios. Si bien algunas técnicas pueden hacer que no sea factible recuperar los datos de destino a través de la interfaz del dispositivo y no se puedan usar para el almacenamiento posterior de datos, el dispositivo no se considera destruido a menos que la recuperación de los datos de destino no sea factible utilizando técnicas de laboratorio de última generación.<br><br>• *Desintegrar, pulverizar, fundir e incinerar*. Estos métodos de desinfección están diseñados para destruir completamente los medios. Por lo general, se llevan a cabo en una instalación de destrucción de metales subcontratada o en una instalación de incineración autorizada con las capacidades específicas para realizar estas actividades de manera efectiva y segura.<br>• *Desgarrar*. Las trituradoras de papel se pueden utilizar para destruir medios flexibles, como disquetes, una vez que los medios se retiran físicamente de sus contenedores exteriores. El tamaño de los fragmentos de basura debe ser lo suficientemente pequeño como para que exista una seguridad razonable, en proporción a la confidencialidad de los datos, de que no se pueden reconstruir. Para dificultar aún más la reconstrucción de los datos, el material triturado se puede mezclar con material no sensible del mismo tipo (por ejemplo, papel triturado o soporte flexible triturado).<br>La aplicación de técnicas destructivas puede ser la única opción cuando los medios fallan y otras técnicas de limpieza o purga no se pueden aplicar de manera efectiva a los medios, o cuando la verificación de los métodos de limpieza o purga falla (por razones conocidas o desconocidas). |

Tabla 5-1 – Métodos de desinfección
(de NIST 800-88, Rev. 1, Directrices para la desinfección de medios)

**Validación**

Las reparticiones deben probar una muestra representativa de los medios para una desinfección adecuada y garantizar que se mantenga la protección adecuada.

**Verificación de equipos**

Si la Repartición está utilizando herramientas de desinfección (por ejemplo, un desmagnetizador), la entidad debe tener procedimientos para garantizar que las herramientas estén funcionando de manera efectiva.

**Verificación de Competencias del Personal**

Las Reparticiones deben garantizar que los operadores de equipos estén adecuadamente capacitados y sean competentes para realizar funciones de desinfección.

**Documento**

Las Reparticiones deben mantener un registro de su desinfección para documentar qué medios se desinfectaron, cuándo, cómo se desinfectaron y la disposición final de los medios.

# 3.0 Cumplimiento

Los empleados que incumplan esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y/o administrativas si correspondieren. Los no empleados, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

# 4.0 Historial de revisiones

| Fecha | Descripción de Cambio | Participantes |
|---|---|---|
| 07/08/2024 | Revision inicial | Alejandro Castro, Pablo Zalazar |
| 08/08/2024 | Visado, y corrección de errores | Alejandro Castro. |

# 5.0 Documentos relacionados

NIST 800-88, Rev. 1, Directrices para la desinfección de medios.

# Capítulo 23

# Política de Protección Física y Ambiental

### 1.0 OBJETIVO

Garantizar que los recursos de Tecnología de la Información (TI) estén protegidos por medidas de seguridad físicas y ambientales que impidan la manipulación física, el daño, el robo o el acceso físico no autorizado.

### 2.0 POLÍTICA

Esta política es aplicable a todos los departamentos y usuarios de recursos y activos de TI.

1. AUTORIZACIONES DE ACCESO FÍSICO
   El Departamento de TI deberá:

   a. Desarrollar, aprobar y mantener una lista de personas con acceso autorizado a las instalaciones donde residen los sistemas de información.

   b. Emitir credenciales de autorización para el acceso a las instalaciones.

   c. Revisar la lista de acceso que detalla el acceso autorizado a las instalaciones por parte de las personas y elimine a las personas de la lista de acceso a las instalaciones cuando el acceso ya no sea necesario.

2. CONTROL DE ACCESO FÍSICO
   El Departamento de TI deberá:

   a. Hacer cumplir las autorizaciones de acceso físico verificando las autorizaciones de acceso individuales antes de otorgar acceso a las instalaciones.

   b. Controlar el ingreso/salida a la instalación usando sistemas/dispositivos y/o medidas de control de acceso físico definidos por la Repartición.

   c. Mantener registros de auditoría de acceso físico para puntos de entrada/salida definidos por la Repartición.

   d. Proporcionar métodos de seguridad definidas por la Repartición para controlar el acceso a áreas dentro de la instalación oficialmente designadas como de acceso público.

   e. Escoltar a los visitantes y monitorear la actividad de los visitantes en áreas especificadas por la Repartición que considere deban tener esta política.

f. Claves seguras, combinaciones y otros dispositivos de acceso físico.

g. Inventario de dispositivos de acceso físico definidos por la Repartición en una frecuencia definida por la Repartición.

h. Cambiar combinaciones y claves en una frecuencia definida por la Repartición y/o cuando se pierden las claves, las combinaciones se ven comprometidas o las personas son transferidas o desvinculadas.

3. PRUEBAS DE PENETRACIÓN DE INSTALACIONES
El Departamento de TI deberá:

a. Emplear un proceso de prueba de penetración que incluya en una frecuencia definida por la Repartición, intentos no anunciados de eludir los controles de seguridad asociados con los puntos de acceso físico a las instalaciones.

4. CONTROL DE ACCESO AL MEDIO DE TRANSMISIÓN
El Departamento de TI deberá:

a. Controlar el acceso físico a líneas de transmisión y distribución del sistema de información definido por la Repartición dentro de las instalaciones de la entidad utilizando métodos de seguridad definidas por la Repartición.

5. CONTROL DE ACCESO PARA DISPOSITIVOS DE SALIDA
El Departamento de TI deberá:

a. Controlar el acceso físico a los dispositivos de salida del sistema de información para evitar que personas no autorizadas obtengan la salida.

Controlar el acceso físico a los dispositivos de salida incluye, por ejemplo, colocar los dispositivos de salida en habitaciones cerradas u otras áreas seguras y permitir el acceso únicamente a personas autorizadas, y colocar los dispositivos de salida en ubicaciones que puedan ser monitoreadas por el personal. Monitores, impresoras, fotocopiadoras, escáneres, máquinas de fax y dispositivos de audio son ejemplos de dispositivos de salida de sistemas de información.

6. MONITOREO DEL ACCESO FÍSICO
El Departamento de TI deberá:

a. Monitorear el acceso físico a las instalaciones donde reside el sistema de información para detectar y responder a incidentes de seguridad física.

b. Revisar los registros de acceso físico en una frecuencia definida por la Repartición y al ocurrir eventos definidos por la Repartición o posibles

indicaciones de eventos; y coordinar los resultados de las revisiones e investigaciones con la capacidad de respuesta a incidentes del Gobierno de Jujuy.

7. REGISTROS DE ACCESO DE VISITANTES
   El Departamento de TI deberá:

   a. Mantener registros de acceso de visitantes a las instalaciones donde reside el sistema de información para un período de tiempo definido por la Repartición; y revisa los registros de acceso de los visitantes en una frecuencia definida por la Repartición.

8. EQUIPOS DE ENERGÍA Y CABLEADO
   El Departamento de TI deberá:

   a. Proteger los equipos eléctricos y el cableado eléctrico del sistema de información contra daños y destrucción.

   b. Determinar los tipos de protección necesarios para los equipos de potencia y cableado empleados en diferentes ubicaciones tanto internas como externas a las instalaciones gubernamentales y entornos de operación. Esto incluye, por ejemplo, generadores y cableado de energía fuera de edificios, cableado interno y fuentes de energía ininterrumpida dentro de una oficina o centro de datos, y fuentes de energía para entidades autónomas como vehículos y satélites.

9. APAGADO DE EMERGENCIA
   El Departamento de TI deberá:

   a. Proporcionar la capacidad de cortar la energía al sistema de información o a los componentes individuales del sistema en situaciones de emergencia.

   b. Colocar interruptores o dispositivos de cierre de emergencia para facilitar el acceso fácil y seguridad del personal; y proteger la capacidad de corte de energía de emergencia contra activaciones no autorizadas.

10. ENERGÍA DE EMERGENCIA

El Departamento de TI deberá:

a. Proporcionar un suministro de energía ininterrumpida de corto plazo para facilitar un apagado ordenado del sistema de información; transición del sistema de información a energía alternativa a largo plazo en caso de una pérdida de la fuente de energía primaria.

b. Proporcionar una fuente de alimentación alternativa a largo plazo para el sistema de información que sea capaz de mantener la capacidad operativa mínima requerida en caso de una pérdida prolongada de la fuente de energía primaria.

11. ILUMINACIÓN DE EMERGENCIA

El Departamento de TI deberá:

a. Emplear y mantener iluminación de emergencia automática para el sistema de información que se activa en caso de un corte o interrupción del suministro eléctrico y que cubra las salidas de emergencia y las rutas de evacuación dentro de la instalación.

b. Proporcionar iluminación de emergencia para todas las áreas dentro de las instalaciones que respalden misiones esenciales y funciones gubernamentales.

12. PROTECCIÓN CONTRA INCENDIOS

El Departamento de TI deberá:

a. Emplear y mantener dispositivos/sistemas de detección y extinción de incendios para el sistema de información que estén respaldados por una fuente de energía independiente.

   Esto se aplica principalmente a instalaciones que contienen concentraciones de recursos de sistemas de información, incluidos, por ejemplo, centros de datos, salas de servidores y salas de computadoras centrales. Los dispositivos/sistemas de detección y extinción de incendios incluyen, por ejemplo, sistemas de rociadores, extintores de incendios portátiles, mangueras fijas contra incendios y detectores de humo.

13. CONTROLES DE TEMPERATURA Y HUMEDAD

El Departamento de TI deberá:

a. Mantener los niveles de temperatura y humedad dentro de las instalaciones donde reside el sistema de información en niveles aceptables definidos por la Repartición.

b. Monitorear los niveles de temperatura y humedad en una frecuencia definida por la Repartición incluir alarmas o notificaciones de cambios potencialmente perjudiciales para el personal o el equipo.

14. PROTECCIÓN CONTRA DAÑOS POR AGUA

El Departamento de TI deberá:

a. Proteger el sistema de información de daños resultantes de fugas de agua proporcionando válvulas maestras de cierre o aislamiento que sean accesibles, funcionen correctamente y sean conocidas por el personal clave.

   Esto se aplica principalmente a instalaciones que contienen concentraciones de recursos de sistemas de información, incluidos, por ejemplo, centros de datos, salas de servidores y salas de computadoras centrales. Se pueden emplear válvulas de aislamiento además de, o en lugar de, válvulas de cierre maestras para cerrar el suministro de agua en áreas específicas de preocupación, sin afectar a las reparticiones.

15. ENTREGA Y RETIRO

El Departamento de TI deberá:

a. Autorizar, monitorear y controlar la entrada y salida de las instalaciones y mantener registros de los artículos entregados y retirados de las instalaciones.

   Hacer cumplir eficazmente las autorizaciones de entrada y salida de los componentes del sistema de información puede requerir restringir el acceso a las áreas de entrega y posiblemente aislar las áreas del sistema de información y las bibliotecas multimedia.

16. SITIO DE TRABAJO ALTERNO

El Departamento de TI deberá:

a. Emplear controles de seguridad definidos por la Repartición en sitios de trabajo alternos.

b. Evaluar, en la medida de lo posible, la efectividad de los controles de seguridad en los sitios de trabajo alternos.

c. Proporcionar un medio para que los empleados se comuniquen con el personal de seguridad de la información en caso de incidentes o problemas de seguridad.

   Los lugares de trabajo alternativos pueden incluir, por ejemplo, otras instalaciones gubernamentales o residencias privadas de empleados. Si bien comúnmente son distintos de los sitios de procesamiento alternativos, los sitios de trabajo alternativos pueden proporcionar ubicaciones alternativas fácilmente disponibles como parte de las operaciones de contingencia. El personal puede

definir diferentes conjuntos de controles de seguridad para sitios de trabajo alternativos específicos o tipos de sitios dependiendo de las actividades relacionadas con el trabajo que se llevan a cabo en esos sitios.

## 3.0 CUMPLIMIENTO

Los empleados que incumplan esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y/o administrativas si correspondieren. Los no empleados, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

## 4.0 EXCEPCIONES DE POLÍTICA

Las solicitudes de excepciones a esta política serán revisadas por el Director de Ciberseguridad (DC) y la Secretaría de Innovación Pública (SIP) y/o Encargado de Seguridad de la Información. Los departamentos que soliciten excepciones deberán proporcionar dichas solicitudes al DC/SIP. La solicitud debe indicar específicamente el alcance de la excepción junto con la justificación para otorgar la excepción, el posible impacto o riesgo asociado al otorgar la excepción, las medidas de mitigación de riesgos que debe tomar el Departamento de TI, iniciativas, acciones y un cronograma para lograrlo, el nivel mínimo de cumplimiento de las políticas aquí establecidas. El DC/SIP revisará dichas solicitudes; consultar con el departamento solicitante.

## 5.0 HISTORIAL DE REVISIONES

| Fecha | Descripción de Cambio | Participantes |
|---|---|---|
| 07/08/2024 | Revisión inicial | Alejandro Castro, Pablo Zalazar |
| 08/08/2024 | Visado, y corrección de errores | Alejandro Castro. |

## 6.0 REFERENCIA

Publicaciones especiales (SP) del Instituto Nacional de Estándares y Tecnología (NIST):NIST SP 800-53a – Protección física y ambiental (PE), NIST SP 800-46, NIST SP 800-73, SP NIST 800-76, SP NIST 800-78, SP NIST 800-116;Directiva de la Comunidad de Inteligencia (ICD):704 705; Departamento de Defensa (DoD): Instrucción 5200.39 Protección de información crítica del programa (CPI); Publicación federal de gestión de identidad, credenciales y acceso (FICAM): Verificación de identidad personal (PIV) en el sistema de control de acceso empresarial (E-PACS) (2012)

# Capítulo 24

# Ciclo de Vida de Desarrollo de Sistemas Seguros

## 1.0 Propósito y Beneficios

Si bien muchos lo consideran un proceso separado, la seguridad de la información es un requisito gubernamental que debe considerarse durante todo el ciclo de vida de desarrollo del sistema (SDLC por su sigla en inglés Software Development Lifecycle). Este Estándar del ciclo de vida del desarrollo de sistemas seguros define los requisitos de seguridad que deben considerarse y abordarse en cada SDLC.

Los sistemas y aplicaciones informáticas se crean para abordar las necesidades gubernamentales. Para hacerlo de manera efectiva, los requisitos del sistema deben identificarse tempranamente y abordarse como parte del SDLC. No identificar un requisito hasta el final del proceso puede tener repercusiones importantes para el éxito de un proyecto y provocar retrasos en la entrega del proyecto, implementación de un sistema inadecuado e incluso el abandono del proyecto. Además, por cada fase por la que pasa un proyecto sin identificar y abordar un requisito, más costoso y lento será solucionar los problemas que surgen debido a la omisión.

La seguridad de la información debe considerarse e integrarse adecuadamente en cada fase del SDLC. No identificar los riesgos e implementar controles adecuados puede resultar en una seguridad inadecuada, lo que podría poner a las entidades en riesgo de sufrir violaciones de datos, exposición a su reputación, pérdida de confianza pública, compromiso de sistemas/redes, sanciones financieras y/o responsabilidad legal.

## 2.0 Declaración de información

La seguridad es un requisito que debe incluirse en cada fase del ciclo de vida del desarrollo de un sistema. El ciclo de vida de desarrollo de un sistema que incluye actividades de seguridad definidas formalmente dentro de sus fases se conoce como SDLC seguro. Según la Política de seguridad de la información, se debe utilizar un SDLC seguro en el desarrollo de todas las aplicaciones y sistemas.

Estas actividades deben estar documentadas o referenciadas dentro de un plan de seguridad de la información asociado. La documentación debe ser suficientemente detallada para demostrar hasta qué punto se aplica cada actividad de seguridad. La documentación debe conservarse para fines de auditoría. Como mínimo, un SDLC debe contener las siguientes actividades de seguridad:

1. Definir roles y responsabilidades de seguridad
2. Orientar al personal sobre las tareas de seguridad del SDLC
3. Establecer un nivel de criticidad del sistema

4. Clasificar información
5. Establecer requisitos de credenciales de identidad del sistema
6. Establecer objetivos del perfil de seguridad del sistema
7. Crear un perfil del sistema
8. Descomponer el sistema
9. Evaluar vulnerabilidades y amenazas
10. Evaluar riesgos
11. Seleccionar y documentar controles de seguridad
12. Crear datos de prueba
13. Probar los controles de seguridad
14. Realizar Certificación y Acreditación
15. Gestionar y controlar el cambio
16. Medir el cumplimiento de la seguridad
17. Realizar la eliminación del sistema

No existe necesariamente una correspondencia uno a uno entre las actividades de seguridad y las fases del SDLC. Las actividades de seguridad a menudo deben realizarse de forma iterativa a medida que un proyecto avanza o recorre el SDLC. A menos que se indique lo contrario, la ubicación de las actividades de seguridad dentro del SDLC puede variar de acuerdo con el SDLC que se utiliza y las necesidades de seguridad de la aplicación o sistema. Apéndice A: Actividades de seguridad dentro del SDLC proporciona un ejemplo de correlación de las actividades de seguridad con un ciclo de vida de desarrollo de sistema genérico. Apéndice B: Descripción de las actividades de seguridad proporciona una descripción de las consideraciones y actividades de seguridad anteriores.

Finalmente, es importante señalar que el proceso SDLC seguro es integral por intención, para garantizar la debida diligencia, el cumplimiento y la documentación adecuada de los controles y consideraciones relacionados con la seguridad. Diseñar la seguridad en los sistemas requiere una inversión de tiempo y recursos. El grado en que se aplica la seguridad al proceso SDLC debe ser proporcional a la clasificación (sensibilidad de los datos y criticidad del sistema) del sistema que se está desarrollando y los riesgos que este sistema puede introducir en el entorno general. Esto asegura valor al proceso de desarrollo y entregable. En términos generales, el mejor retorno de la inversión se logra aplicando rigurosamente la seguridad dentro del proceso SDLC a proyectos de alto riesgo y alto costo. Cuando se determina que un proyecto no aprovechará todo el proceso SDLC seguro (por ejemplo, en un proyecto de menor riesgo/costo), se debe documentar la justificación y las actividades de seguridad que no se utilizan deben identificarse y aprobarse como parte del proceso formal de aceptación de riesgos.

Nota: La clasificación de datos no se puede utilizar como único factor determinante de si el proyecto es o no de bajo riesgo/costo. Por ejemplo, los sitios web públicos no pueden considerarse proyectos de bajo riesgo/costo incluso si todos los datos son públicos. Existe el riesgo de que el sitio web se vea comprometido al inyectar malware

y comprometer las máquinas de los visitantes o al cambiar el contenido del sitio web para afectar la reputación de la administración pública.

## 3.0 Cumplimiento

Los empleados que violen esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y/o administrativas si correspondieren. Los no empleados, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

## 4.0 Historial de revisiones

| Fecha | Descripción de Cambio | Crítico |
|---|---|---|
| | | |

## 5.0 Documentos relacionados

Publicación especial del NIST 800-30, Guía para realizar evaluaciones de riesgos

Publicación especial del NIST 800-53, Controles de seguridad y privacidad para organizaciones y sistemas de información federales

Publicación especial del NIST 800-53A, Guía para evaluar los controles de seguridad en organizaciones y sistemas de información: creación de planes de evaluación eficaces

Apéndice A: Actividades de seguridad dentro del SDLC

La siguiente tabla muestra la ubicación de las actividades de seguridad dentro de las fases de un SDLC de muestra. La ubicación real de las actividades de seguridad dentro del ciclo de vida de desarrollo del sistema puede variar de acuerdo con el SDLC real que se utiliza en un proyecto y las necesidades de seguridad particulares de la aplicación o sistema. Las publicaciones del NIST en la tercera columna de esta tabla son documentos recomendados para brindar orientación en la ubicación y ejecución de tareas de seguridad dentro del ciclo de vida de desarrollo del sistema. Estos documentos están disponibles en el sitio web del NIST (http://csrc.nist.gov/publications/PubsSPs.html).

Figura A-1: Ubicación de las actividades de seguridad dentro de las fases del SDLC

| **PMG del estado de Nueva York Fase SDLC** | **Actividad de seguridad** | **Publicaciones del NIST** |
|---|---|---|
| Iniciación del sistema | • Definir roles y responsabilidades de seguridad<br>• Orientar al personal sobre las tareas de seguridad del SDLC<br>• Establecer un nivel de criticidad del sistema<br>• Clasificar información (preliminar)<br>• Establecer requisitos de nivel de garantía del sistema<br>• Establecer objetivos del perfil de seguridad del sistema (preliminar)<br>• Crear un perfil del sistema (preliminar) | • SP800-12<br>• SP800-14<br>• SP800-35<br>• SP800-27<br>• SP800-47<br>• SP800-60<br>• SP800-63<br>• FIPS 199 |
| Análisis de requisitos del sistema | • Establecer objetivos del perfil de seguridad del sistema (iterativo)<br>• Clasificar información (iterativo)<br>• Descomponer el sistema (preliminar) | • SP800-23<br>• SP800-30<br>• SP800-36<br>• SP800-53<br>• SP800-55<br>• SP800-64<br>• FIPS 140-2 |
| Diseño de sistemas | • Crear un perfil del sistema (iterativo)<br>• Descomponer el sistema (iterativo)<br>• Evaluar vulnerabilidades y amenazas (preliminar)<br>• Evaluar riesgos (preliminar)<br>• Seleccionar y documentar controles de seguridad (preliminares) | |
| Construcción del sistema | • Crear datos de prueba<br>• Evaluar vulnerabilidades y amenazas (iterativo)<br>• Evaluar riesgos (iterativo)<br>• Seleccionar y documentar controles de seguridad (iterativo)<br>• Probar controles de seguridad | • SP800-35<br>• SP800-36<br>• SP800-37<br>• SP800-51<br>• SP800-53<br>• SP800-53A |

Apéndice A: Actividades de seguridad dentro del SDLC

| **PMG del estado de Nueva York Fase SDLC** | **Actividad de seguridad** | **Publicaciones del NIST** |
|---|---|---|
| Implementación del sistema | • Medir el cumplimiento de la seguridad<br>• Perfil de seguridad del sistema de documentos<br>• Requisitos y controles de seguridad de documentos | • SP800-55<br>• SP800-56<br>• SP800-57<br>• SP800-61<br>• SP800-64 |
| Aceptación del sistema | • Realizar la Certificación y Acreditación del Sistema | |
| Operaciones y mantenimiento | • Medir el cumplimiento de la seguridad (periódico)<br>• Gestionar y controlar el cambio<br>• Realizar Certificación y Acreditación del Sistema (iterativo) | • SP800-26<br>• SP800-31<br>• SP800-34<br>• SP800-37<br>• SP800-53A<br>• SP800-55 |
| Disposición | • Preservar la información<br>• Desinfectar los medios<br>• Deseche el hardware y el software | • SP800-12<br>• SP800-14<br>• SP800-35<br>• SP800-36<br>• SP800-64 |

1. Definir roles y responsabilidades de seguridad

Se deben definir roles de seguridad y cada actividad de seguridad dentro del SDLC debe asignarse claramente a uno o más roles de seguridad. Estos roles deben estar documentados e incluir a las personas responsables de las actividades de seguridad asignadas a cada rol. Apéndice C: Roles de seguridad dentro del SDLC proporciona pautas para definir roles de seguridad y asignar actividades de seguridad a roles.

2. Orientar al personal sobre las tareas de seguridad del SDLC

Todas las partes involucradas en la ejecución de las actividades de seguridad del SDLC de un proyecto o política pública deben comprender el propósito, los objetivos y los entregables de cada actividad de seguridad en la que participan o de la que son responsables.

3. Establecer el nivel de criticidad del sistema

Al iniciar una aplicación o sistema, se debe establecer la criticidad del sistema. El nivel de criticidad debe reflejar el valor gubernamental de la función proporcionada por el sistema y el daño potencial que podría resultar de una pérdida de acceso a esta funcionalidad.

4. Clasificar información

Según la Política de Seguridad informática, toda la información contenida, manipulada o que pase por un sistema o aplicación debe estar clasificada. La clasificación debe reflejar la importancia de la confidencialidad, integridad y disponibilidad de la información.

5. Establecer requisitos de credenciales de identidad del sistema

Todas las aplicaciones o sistemas que requieran autenticación deben establecer una credencial de identidad de usuario. La credencial de identidad debe reflejar el nivel de confianza requerido de que la persona que intenta acceder al sistema es quien dice ser y el posible impacto en la seguridad e integridad del sistema si la persona no es quien dice ser.

6. Establecer objetivos del perfil de seguridad del sistema

Al iniciar una aplicación o sistema, se deben identificar y documentar los objetivos del perfil de seguridad. Estos objetivos deben establecer la importancia y relevancia de los conceptos de seguridad identificados (Apéndice D: Conceptos de seguridad) al sistema e indicar el alcance y el rigor con el que cada concepto de seguridad debe incorporarse o reflejarse en el sistema y el software. Cada concepto de seguridad debe considerarse a lo largo de cada fase del ciclo de vida y se debe documentar cualquier consideración o necesidad especial.

El propósito detrás de establecer perfiles de seguridad del sistema y monitorearlos a lo largo del ciclo de vida es ser consciente de la prioridad relativa, el peso y la relevancia de cada concepto de seguridad en cada fase del ciclo de vida del sistema. Las entidades deben verificar que los objetivos del perfil de seguridad consideren adecuadamente todos los mandatos de seguridad nacionales, provinciales y externos que el sistema debe cumplir.

7. Perfilar el sistema

El sistema o aplicación que se está desarrollando debe ser perfilado iterativamente por equipos técnicos dentro del SDLC. Un perfil de sistema es una descripción general de alto nivel de la aplicación que identifica los atributos de la aplicación, como la topología física, los niveles lógicos, los componentes, los servicios, los actores, las tecnologías, las dependencias externas y los derechos de acceso. Este perfil deberá actualizarse a lo largo de las distintas fases del SDLC.

8. Descomponer el sistema

El sistema o aplicación debe descomponerse en componentes más finos y su mecánica (es decir, el funcionamiento interno) debe documentarse. Esta actividad se realizará de forma iterativa dentro del SDLC. La descomposición incluye la identificación de límites de confianza, puntos de entrada y salida de información, flujos de datos y códigos privilegiados.

9. Evaluar vulnerabilidades y amenazas

Las evaluaciones de vulnerabilidad deben realizarse de forma iterativa dentro del proceso SDLC. Las evaluaciones de amenazas deben considerar no solo las amenazas técnicas, sino también las administrativas y físicas que podrían tener un impacto negativo potencial en la confidencialidad, disponibilidad e integridad del sistema. Las evaluaciones de amenazas deben considerar y documentar las fuentes de amenazas, las motivaciones de las fuentes de amenazas y los métodos de ataque que potencialmente podrían representar amenazas a la seguridad del sistema.

Las evaluaciones de amenazas deben cumplir con todos los mandatos nacionales y provinciales relevantes que la Repartición debe cumplir y seguir las mejores prácticas globales, incluida la documentación de los procesos de evaluación. Las evaluaciones de amenazas y los resultados del modelado de amenazas subyacentes que respaldan la evaluación también deben estar completamente documentados. Apéndice E: Recursos para la evaluación de amenazas y riesgos incluye una lista de recursos recomendados para realizar evaluaciones de amenazas.

10. Evaluar el riesgo

Las evaluaciones de riesgos deben realizarse de forma iterativa dentro del proceso SDLC. Estos comienzan como un proceso informal de alto nivel al comienzo del SDLC y se convierten en un proceso formal e integral antes de poner un sistema o software en producción.

Las amenazas y vulnerabilidades identificadas en las evaluaciones de amenazas deben abordarse en las evaluaciones de riesgos. Las evaluaciones de riesgos deben basarse en el valor de la información en el sistema, la clasificación de la información, el valor de la función gubernamental proporcionada por el sistema, las amenazas potenciales al sistema, la probabilidad de que ocurra, el impacto de la falla del sistema y las consecuencias del fallo de los controles de seguridad.

Los riesgos identificados deben gestionarse adecuadamente evitando, transfiriendo, aceptando o mitigando el riesgo. Está prohibido ignorar el riesgo. Las evaluaciones de riesgos deben cumplir con todos los mandatos nacionales y provinciales relevantes que la Repartición debe documentar y cumplir.

Las evaluaciones de riesgos deben revisarse y actualizarse periódicamente según sea necesario cada vez que se modifique la evaluación de la amenaza subyacente o cuando se realicen cambios significativos en el sistema. Apéndice E: Recursos para la evaluación de amenazas y riesgos incluye una lista de recursos recomendados para realizar evaluaciones de riesgos.

11. Seleccionar y documentar controles de seguridad

Se deben implementar controles de seguridad adecuados para mitigar los riesgos que no se evitan, transfieren o aceptan. Los controles de seguridad deben justificarse y documentarse con base en las evaluaciones de riesgos, las evaluaciones de amenazas y el análisis del costo de implementar un control de seguridad potencial en relación con la disminución del riesgo que se logra al implementar el control.

La documentación de los controles debe ser lo suficientemente detallada para permitir la verificación de que todos los sistemas y aplicaciones cumplen con las políticas de seguridad

relevantes y para responder eficientemente a nuevas amenazas que puedan requerir modificaciones a los controles existentes.
El riesgo residual debe documentarse y mantenerse en niveles aceptables. Se debe realizar una aceptación formal del riesgo, con la aprobación del CISO o responsable de seguridad, para los riesgos medianos y altos que persisten después de que se hayan implementado los controles de mitigación.
Los requisitos de control de seguridad deben revisarse y actualizarse periódicamente según sea necesario cada vez que se modifique el sistema o la evaluación de riesgos subyacente.

12. Crear datos de prueba

Se debe crear un proceso para el desarrollo de datos de prueba significativos para todas las aplicaciones. Debe haber un proceso de prueba disponible para que las aplicaciones realicen pruebas de seguridad y regresión.
Los datos de producción confidenciales no deben utilizarse con fines de prueba. Si se utilizan datos de producción, las Reparticiones deben cumplir con las políticas y estándares nacionales y provinciales y externos aplicables con respecto a la protección y eliminación de datos de producción.

13. Probar los controles de seguridad

Los controles deben probarse minuciosamente en entornos de preproducción que sean idénticos, en la medida de lo posible, al entorno de producción correspondiente. Esto incluye el hardware, el software, las configuraciones del sistema, los controles y cualquier otra personalización.
El proceso de prueba, incluidas las pruebas de regresión, debe demostrar que los controles de seguridad se han aplicado correctamente, se han implementado y están funcionando correctamente y contrarrestando las amenazas y vulnerabilidades para las que están destinados. El proceso de prueba también debe incluir pruebas de vulnerabilidad y demostrar la corrección de vulnerabilidades críticas antes de poner el sistema en producción.
Se debe observar una separación adecuada de funciones a lo largo de los procesos de prueba, como garantizar que diferentes personas sean responsables del desarrollo, el control de calidad y la acreditación.

14. Realizar Acreditación

El plan de seguridad del sistema debe ser analizado, actualizado y aceptado por la Director de Ciberseguridad (DC) o responsable de seguridad).

15. Gestionar y controlar el cambio

Se debe seguir un proceso formal de gestión de cambios cada vez que se modifica un sistema o aplicación para evitar impactos negativos directos o indirectos que el cambio pueda imponer. El proceso de gestión de cambios debe garantizar que las actividades de seguridad del SDLC se consideren y realicen, si corresponde, y que los controles y documentación de seguridad del SDLC que se vean afectados por el cambio estén actualizados.

16. Medir el cumplimiento de la seguridad

Las aplicaciones y sistemas deben someterse a evaluaciones periódicas de cumplimiento de seguridad para garantizar que reflejen una postura de seguridad acorde con la definición de riesgo aceptable. Las evaluaciones del cumplimiento de la seguridad deben incluir evaluaciones del cumplimiento de los estándares de cumplimiento nacionales y provinciales y externos que la Repartición debe cumplir.

Las evaluaciones del cumplimiento de la seguridad deben realizarse después de los cambios en el sistema y las aplicaciones y periódicamente como parte del monitoreo continuo del cumplimiento del sistema.

17. Realizar la eliminación del sistema

La información contenida en aplicaciones y sistemas debe protegerse una vez que un sistema haya llegado al final de su vida útil. La información debe conservarse de acuerdo con los mandatos nacionales y provinciales aplicables u otros requisitos de retención. La información sin requisitos de retención debe descartarse o destruirse y los medios desechados deben desinfectarse de acuerdo con los estándares nacionales y provinciales aplicables para eliminar la información residual.

Apéndice C: Roles de seguridad dentro del SDLC

La responsabilidad de cada actividad de seguridad dentro del SDLC se debe asignar a uno o más roles de seguridad. Para lograr esto, la definición predeterminada de una función SDLC se puede ampliar para incluir responsabilidades de seguridad y/o se pueden definir nuevas funciones de seguridad para abarcar actividades de seguridad. En todos los casos, la asignación de funciones de las actividades de seguridad y la identificación de las personas a las que se les asigna la responsabilidad de dichas funciones deben estar claramente documentadas.

Con el fin de utilizar una definición coherente de funciones en varios SDLC, se recomienda encarecidamente que las Reparticiones utilicen como directrices las publicaciones del Instituto Nacional de Estándares y Tecnología (NIST). De relevancia específica para la definición de roles y marcos de SDLC son:

- Publicación especial del NIST 800-37 Rev. 2 Marco de gestión de riesgos para organizaciones y sistemas de información: un enfoque del ciclo de vida del sistema para la seguridad y la privacidad

La composición de un sistema y software desde una perspectiva de seguridad es su perfil de seguridad e incluye los siguientes conceptos de seguridad, que deben considerarse y documentarse como parte de un proceso SDLC seguro.

Figura D-1: Conceptos de seguridad

| **Concepto** | **Descripción** |
|---|---|
| Confidencialidad | Proteger contra la divulgación de información no autorizada |
| Integridad | Proteger contra modificaciones no autorizadas, involuntarias o incorrectas de software o datos. |
| Disponibilidad | Garantizar la disponibilidad de los sistemas y la información. |
| Autenticación | El proceso de establecer confianza en la identidad de los usuarios o sistemas de información. |
| Autorización | Establecer derechos de acceso a los recursos. |
| Auditoría/Registro | Crear un registro histórico de las acciones de los usuarios y de los procesos críticos del sistema. |
| Gestión de sesiones | Asegurar de que una sesión mantenga la confidencialidad y la integridad de la información intercambiada entre un sistema y un usuario autenticado. |
| Gestión de errores y excepciones | Asegurar de que el comportamiento involuntario y poco confiable del sistema se maneje de forma segura. Esto ayuda a garantizar la protección contra amenazas a la confidencialidad, la integridad y la disponibilidad. |
| Gestión de parámetros de configuración | Asegurar de que los parámetros configurables necesarios para que se ejecute el software o un sistema estén adecuadamente protegidos. |
| Privilegios mínimos | Asignar sólo los derechos mínimos permitidos a un sujeto que solicita acceso a un recurso durante el menor tiempo necesario. |
| Separación de privilegios | Asegurar de que se cumplan varias condiciones antes de otorgar permisos a un objeto. |
| Defensa en profundidad | Colocar capas de defensas de seguridad en una aplicación para reducir la posibilidad de un ataque exitoso. |
| Fallar de forma segura | Asegurar de que la confidencialidad y la integridad de un sistema permanezcan intactas incluso aunque se haya perdido la disponibilidad del sistema debido a una falla del sistema. |
| Economía de mecanismos | Mantener la implementación y el diseño del sistema lo más simple posible. |
| Mediación Completa | Requerir comprobaciones de acceso a un objeto cada vez que un sujeto solicite acceso, especialmente para objetos críticos para la seguridad. |
| Diseño abierto | Utilizar mecanismos de protección reales para proteger la información confidencial; no confíe en un diseño o implementación confiables para proteger la información (también conocido como “seguridad a través de la oscuridad”). |
| Mecanismos menos comunes | Evitar que varios sujetos compartan mecanismos para otorgar acceso a un recurso. |

| Concepto | Descripción |
|---|---|
| Aceptabilidad psicológica | Asegurar de que la funcionalidad de seguridad sea fácil de usar y transparente para el usuario. |
| Aprovechar los componentes existentes | Promover la reutilización de componentes existentes. Reutilizar código probado y validado y bibliotecas estándar en lugar de crear código personalizado. |
| Eslabón más débil | Identificar y proteger los componentes más débiles de un sistema. |
| Punto único de fallo | Eliminar cualquier fuente única de compromiso total. |

La información relativa a estos conceptos está disponible públicamente en el sitio web patrocinado por la Oficina de Seguridad Cibernética y Comunicaciones del Departamento de Seguridad Nacional (DHS) de EE. UU. En https://buildsecurityin.us-cert.gov.
Para garantizar la alineación con los mandatos de cumplimiento gubernamental y ayudar a asegurar la prestación eficiente y efectiva de servicios de seguridad, se recomienda el uso de estándares reconocidos globalmente relacionados con marcos basados en riesgos y prácticas seguras del ciclo de vida del desarrollo de sistemas.
En particular, se recomienda encarecidamente el uso de los estándares NIST, especialmente para entidades que deben cumplir con mandatos de seguridad nacionales. Las siguientes publicaciones del NIST brindan orientación recomendada para implementar marcos de gestión de riesgos y realizar evaluaciones de riesgos y amenazas.

- Publicación especial del NIST 800-39, Gestión del riesgo de seguridad de la información: organización, misión y vista del sistema de información
- Publicación especial del NIST 800-37 Rev. 2 Marco de gestión de riesgos para organizaciones y sistemas de información: un enfoque del ciclo de vida del sistema para la seguridad y la privacidad
- Publicación especial del NIST 800-30, Guía para realizar evaluaciones de riesgos
- Publicación especial del NIST 800-53, Controles de seguridad y privacidad para organizaciones y sistemas de información federales
- Publicación especial del NIST 800-53A, Guía para evaluar los controles de seguridad en organizaciones y sistemas de información: creación de planes de evaluación eficaces

Las publicaciones del NIST están disponibles en el sitio web del Instituto Nacional de Estándares y Tecnología (http://csrc.nist.gov/publications/PubsSPs.html).

# Capítulo 25

# Política de Respuesta a amenazas de seguridad informática

### 1.0 OBJETIVO

El propósito de esta política es definir la responsabilidad de la Repartición en la respuesta a amenazas de seguridad que afecten la confidencialidad, integridad y/o disponibilidad de los recursos de tecnología de la información (TI).

### 2.0 POLÍTICA

Esta política es aplicable a todos los departamentos y todos los sistemas de información.

1. RESPUESTA DE EMERGENCIA INFORMÁTICA

    a. Se establecerá un Equipo de Respuesta a Emergencias Informáticas (EREI). El EREI estará dirigido por el Director de Ciberseguridad (DC) o quien designe el MPEyM

    b. El EREI estará compuesto por representantes de todas las Unidades de Organización.

    c. El EREI deberá comunicar información de seguridad, pautas para los procesos de notificación, identificar posibles riesgos de seguridad y coordinar respuestas para frustrar, mitigar o eliminar amenazas de seguridad a los recursos de TI.

    d. Tras la activación de EREI por parte del DC, todos los responsables de Seguridad de la Información y otros representantes de EREI deberán informar directamente al DC durante la activación de EREI.

2. RESPUESTA DE EMERGENCIA INFORMÁTICA
   Cada Repartición establecerá el/los responsable/s de la repartición designados para responder a incidentes y/o coordinar la respuesta a las amenazas de seguridad a los recursos de TI dentro de la Unidad de Organización.

### 3.0 CUMPLIMIENTO

Los empleados que incumplan esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y/o administrativas si correspondieren. Los no empleados, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de

acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

## 4.0 EXCEPCIONES DE POLÍTICA

Las solicitudes de excepciones a esta política serán revisadas por el Director de Ciberseguridad (DC) y Secretaría de Innovación Pública (SIP) y/o Encargado de Seguridad de la Información. Los departamentos que soliciten excepciones deberán proporcionar dichas solicitudes al DC/SIP. La solicitud debe indicar específicamente el alcance de la excepción junto con la justificación para otorgar la excepción, el posible impacto o riesgo asociado al otorgar la excepción, las medidas de mitigación de riesgos que debe tomar el Departamento de TI, iniciativas, acciones y un cronograma para lograrlo, el nivel mínimo de cumplimiento de las políticas aquí establecidas. El DC/SIP revisará dichas solicitudes; consultar con el departamento solicitante.

## 5.0 HISTORIAL DE REVISIONES

| Fecha | Descripción de Cambio | Participantes |
|---|---|---|
| 09/08/2024 | Revisión inicial | Alejandro Castro, Pablo Zalazar |
| 12/08/2024 | Visado, y corrección de errores | Alejandro Castro. |

## 6.0 REFERENCIA

Publicación especial (SP) del Instituto Nacional de Estándares y Tecnología (NIST): NIST SP 800-61: Guía de manejo de incidentes de seguridad informática

# Capítulo 26

# Política de Planificación de Contingencias

### 1.0 OBJETIVO

Garantizar que los recursos y sistemas de información normales de tecnología de la información (TI) estén disponibles durante momentos de interrupción de los servicios.

### 2.0 POLÍTICA

Esta política es aplicable a todos los departamentos y usuarios de recursos y activos de TI.

1. PLAN DE CONTINGENCIA
   El Departamento de TI deberá:

   a. Desarrollar un plan de contingencia para el sistema de información, en orientación directa y asociación con el propietario del sistema de información, que:

      i. Identifica misiones esenciales y funciones gubernamentales y requisitos de contingencia asociados.

      ii. Proporciona objetivos de recuperación, prioridades de restauración y métricas.

      iii. Aborda roles de contingencia, responsabilidades, personas asignadas con información de contacto.

      iv. Aborda el mantenimiento de misiones esenciales y funciones gubernamentales a pesar de una interrupción, compromiso o falla del sistema de información.

      v. Aborda la eventual restauración completa del sistema de información sin deterioro de los controles de seguridad originalmente planificados e implementados.

      vi. Es revisado y aprobado por el personal o roles definidos por la Repartición y la gestión del propietario del sistema de información al menos una vez al año.

   b. Distribuir copias de los planes de contingencia al personal clave de contingencia, identificado por nombre y/o por función gubernamental.

c. Coordinar las actividades de planificación de contingencias con las actividades de manejo de incidentes.

d. Actualizar el plan de contingencia para abordar los cambios en la misión, el sistema de información o el entorno de operación del responsable de la Repartición y los problemas encontrados durante la implementación, ejecución o prueba del plan de contingencia.

e. Comunicar los cambios del plan de contingencia al personal clave de contingencia identificado por nombre y/o por función comercial.

f. Proteger el plan de contingencia de divulgación y modificación no autorizadas.

2. ENTRENAMIENTO DE CONTINGENCIA
El Departamento de TI deberá:

a. Proporcionar capacitación de contingencia a los usuarios del sistema de información de acuerdo con las funciones y responsabilidades asignadas.

b. Asegurar que el personal designado reciba capacitación para contingencias al menos una vez al año al asumir un rol o responsabilidad de contingencias, y cuando lo requieran cambios en el sistema de información.

3. PRUEBAS DEL PLAN DE CONTINGENCIA
TI, junto con los propietarios de los sistemas de información, deberá:

a. Probar el plan de contingencia para el sistema de información, según lo determine la naturaleza crítica de la misión de los sistemas gubernamentales al menos una vez al año.

b. Utilizar la planificación estratégica y táctica durante las pruebas para simular un sistema de información de producción para determinar la efectividad del plan y la preparación organizacional para ejecutar el plan.

c. Revisar los resultados de las pruebas del plan de contingencia.

d. Iniciar acciones correctivas, según sea necesario.

e. Coordinar las pruebas del plan de contingencia con los elementos organizacionales responsables de los planes relacionados; Los planes de contingencia para sistemas de información incluyen, por ejemplo, planes de continuidad del negocio, de recuperación de desastres, de continuidad de operaciones, de comunicación de crisis, de infraestructura crítica, de respuesta a incidentes cibernéticos y de emergencia para ocupantes.

4. SITIO DE ALMACENAMIENTO ALTERNO

TI, en orientación directa y asociación con el propietario del sistema de información, deberá:

a. Establecer un sitio de almacenamiento alternativo que incluya los acuerdos necesarios para permitir el almacenamiento y la recuperación de información de respaldo del sistema de información.

b. Asegurar que el sitio de almacenamiento alternativo proporcione controles de seguridad de la información equivalentes a las del sitio principal.

c. Identificar un sitio de almacenamiento alternativo que esté separado del sitio de almacenamiento principal para reducir la susceptibilidad a las mismas amenazas.

d. Identificar y documentar posibles problemas de accesibilidad al sitio de almacenamiento alternativo en caso de una interrupción o desastre en toda el área y describa acciones de mitigación explícitas.

5. SITIO DE PROCESAMIENTO ALTERNO
TI, en orientación directa y asociación con el propietario del sistema de información, deberá:

a. Establecer un sitio de procesamiento alternativo que incluya los acuerdos necesarios para permitir la transferencia y reanudación de las operaciones del sistema de información para misiones/funciones gubernamentales esenciales dentro del período de tiempo consistente con los objetivos de tiempo y punto de recuperación cuando las capacidades de procesamiento primario no estén disponibles.

b. Asegurar que los equipos y suministros necesarios para transferir y reanudar las operaciones estén disponibles en el sitio de procesamiento alternativo o que existan contratos para respaldar la entrega al sitio dentro del período de tiempo acordado para la transferencia/reanudación.

c. Asegurar que el sitio de procesamiento alternativo proporcione controles de seguridad de la información equivalentes a las del sitio principal.

d. Identificar un sitio de procesamiento alternativo que esté separado del sitio de procesamiento principal para reducir la susceptibilidad a las mismas amenazas.

e. Identificar posibles problemas de accesibilidad al sitio de procesamiento alternativo en caso de una interrupción o desastre en toda el área y describa acciones de mitigación explícitas.

f. Desarrollar acuerdos de sitios de procesamiento alternativos que contengan disposiciones de prioridad de servicio de acuerdo con los objetivos gubernamentales y los requisitos de disponibilidad.

6. SERVICIOS DE TELECOMUNICACIONES
   El Departamento de TI deberá:

   a. Establecer servicios de telecomunicaciones alternativos, incluidos los acuerdos necesarios para permitir la reanudación de las operaciones del sistema de información para misiones esenciales y funciones gubernamentales dentro de los plazos de recuperación acordados cuando las capacidades de telecomunicaciones primarias no estén disponibles en los sitios de procesamiento o almacenamiento primarios o alternativos.

   b. Desarrollar acuerdos de servicios de telecomunicaciones primarios y alternativos que contengan disposiciones de prioridad de servicio de acuerdo con los objetivos de recuperación y los requisitos de disponibilidad acordados.

   c. Solicitar prioridad de servicio de telecomunicaciones para los servicios de telecomunicaciones utilizados para emergencias de seguridad provincial en el caso de que los servicios de telecomunicaciones primarios y/o alternativos sean proporcionados por un proveedor común.

7. RESPALDO DEL SISTEMA DE INFORMACIÓN
   TI, en orientación directa y asociación con el propietario del sistema de información, deberá:

   a. Realizar copias de seguridad de la información a nivel de usuario contenida en el sistema de información definida por frecuencia consistente con el tiempo de recuperación y los objetivos de punto de recuperación.

   b. Realizar copias de seguridad de la información a nivel del sistema contenida en el sistema de información definida por frecuencia consistente con el tiempo de recuperación y los objetivos del punto de recuperación.

   c. Realizar copias de seguridad de la documentación del sistema de información, incluida la documentación relacionada con la seguridad, definida por frecuencia coherente con el tiempo de recuperación y los objetivos de punto de recuperación.

   d. Proteger la confidencialidad, integridad y disponibilidad de la información de respaldo en las ubicaciones de almacenamiento.

   e. Probar la información de respaldo para verificar la confiabilidad de los medios y la integridad de la información.

8. RECUPERACIÓN Y RECONSTITUCIÓN DEL SISTEMA DE INFORMACIÓN
   TI, en orientación directa y asociación con el propietario del sistema de información, deberá:

a. Proporcionar la recuperación y reconstitución del sistema de información a un estado conocido después de una interrupción, compromiso o falla.

b. Disponer que el sistema de información implemente la recuperación de transacciones para los sistemas que estén basados en transacciones.

## 3.0 CUMPLIMIENTO

Los empleados que incumplan esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y/o administrativas si correspondieren. Los no empleados, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

## 4.0 EXCEPCIONES DE POLÍTICA

Las solicitudes de excepciones a esta política serán revisadas por el Director de Ciberseguridad (DC) y Secretaría de Innovación Pública (SIP), y/o Encargado de Seguridad de la Información. Los departamentos que soliciten excepciones deberán proporcionar dichas solicitudes al DC/SIP. La solicitud debe indicar específicamente el alcance de la excepción junto con la justificación para otorgar la excepción, el posible impacto o riesgo asociado al otorgar la excepción, las medidas de mitigación de riesgos que debe tomar el Departamento de TI, iniciativas, acciones y un cronograma para lograrlo, el nivel mínimo de cumplimiento de las políticas aquí establecidas. El DC/SIP revisará dichas solicitudes; consultar con el departamento solicitante.

## 5.0 HISTORIAL DE REVISIONES

| Fecha | Descripción de Cambio | Participantes |
|---|---|---|
| 09/08/2024 | Revisión inicial | Alejandro Castro, Pablo Zalazar |
| 12/08/2024 | Visado, y corrección de errores | Alejandro Castro. |

## 6.0 REFERENCIA

Publicaciones especiales (SP) del Instituto Nacional de Estándares y Tecnología (NIST): NIST SP 800-53a – Planificación de contingencias (CP), NIST SP 800-16, NIST SP 800-34, NIST SP 800-50, NIST SP 800-84; Estándares federales de procesamiento de información (FIPS) 199 del NIST

# Capítulo 27

# Política de Respuesta a Incidentes

### 1.0 OBJETIVO

Garantizar que la Tecnología de la Información (TI) identifique, contenga, investigue, solucione, informe y responda adecuadamente a los incidentes de seguridad informática.

### 2.0 POLÍTICA

Esta política es aplicable a todos los departamentos y usuarios de recursos y activos de TI.

1. ENTRENAMIENTO DE RESPUESTA A INCIDENTES
   La Repartición con el acompañamiento del MPEYM debe:

   a. Proporcionar capacitación en respuesta a incidentes a los usuarios del sistema de información de acuerdo con las funciones y responsabilidades asignadas:

      i. Dentro de un período de tiempo definido por la Repartición de asumir un rol o responsabilidad de respuesta a incidentes.

      ii. Cuando lo requieran cambios en el sistema de información, y en una frecuencia definida por la Repartición después de eso.

   b. Incorporar eventos simulados en la capacitación de respuesta a incidentes para facilitar una respuesta efectiva por parte del personal en situaciones de crisis.

   c. Emplear mecanismos automatizados para proporcionar un entorno de capacitación de respuesta a incidentes más completo y realista.

2. PRUEBAS DE RESPUESTA A INCIDENTES
   La Repartición debe:

   a. Probar la capacidad de respuesta a incidentes del sistema de información. En una frecuencia definida por la Repartición usando una asignación de pruebas definidas por Repartición para determinar la efectividad de la respuesta al incidente y documentar los resultados.
   b. Coordinar las pruebas de respuesta a incidentes con los contactos de la Repartición responsables de los planes relacionados: de continuidad del negocio, de contingencia, de recuperación de desastres, de continuidad de operaciones, de comunicación de crisis, de infraestructura crítica y de emergencia para ocupantes.

3. MANEJO DE INCIDENTES
   La Repartición debe:

   a. Implementar una capacidad de manejo de incidentes de seguridad que incluya preparación, detección y análisis, contención, erradicación y recuperación.

   b. Coordinar las actividades de manejo de incidentes con las actividades de planificación de contingencias.

   c. Incorporar las lecciones aprendidas de las actividades de manejo de incidentes en curso en los procedimientos de respuesta a incidentes, capacitación y pruebas/ejercicios, e implementar los cambios resultantes en consecuencia.

4. SEGUIMIENTO DE INCIDENTES
   La Repartición debe:

   a. Emplear mecanismos automatizados para ayudar en el seguimiento de incidentes de seguridad y en la recopilación y análisis de información sobre incidentes.

5. INFORME DE INCIDENTE
   La Repartición debe:

   a. Exigir al personal que informe los incidentes de seguridad sospechosos a la capacidad de respuesta a incidentes dentro de un período de tiempo definido por la Repartición. Se sugiere que sea de manera inmediata y hasta dentro de las **primeras 24 horas**.

   b. Reportar información sobre incidentes de seguridad a las autoridades o encargados definidos por la Repartición.

6. ASISTENCIA DE RESPUESTA A INCIDENTES
   La Repartición debe:

   a. Proporcionar un recurso de soporte de respuesta a incidentes, integral a la capacidad de respuesta a incidentes, que ofrezca asesoramiento y asistencia a los usuarios del sistema de información para el manejo y notificación de incidentes de seguridad.

7. PLAN DE RESPUESTA A INCIDENTES
   La Repartición debe:

   a. Desarrollar un plan de respuesta a incidentes en donde:

i. La Repartición proporcione una hoja de ruta para implementar su capacidad de respuesta a incidentes.

ii. Describa la estructura de la capacidad de respuesta a incidentes.

iii. Proporcione un enfoque de alto nivel sobre cómo la capacidad de respuesta a incidentes encaja en el sistema general de la Repartición.

iv. Cumpla con los requisitos únicos de la Repartición, que se relacionan con la misión, el tamaño, la estructura y las funciones.

v. Defina incidentes reportables.

vi. Proporcione métricas para medir la capacidad de respuesta a incidentes dentro de la Repartición.

vii. Defina los recursos y el apoyo de gestión necesarios para mantener y madurar eficazmente una capacidad de respuesta a incidentes.

viii. Sea revisado y aprobado por el personal o roles definidos por la Repartición.

b. Distribuir copias del plan de respuesta a incidentes al personal de respuesta a incidentes definido por la Repartición (identificado por nombre y/o por función).

c. Revisar el plan de respuesta a incidentes en una frecuencia definida por la Repartición.

d. Actualizar el plan de respuesta a incidentes para abordar los cambios del sistema o los problemas encontrados durante la implementación, ejecución o prueba del plan.

e. Comunicar los cambios en el plan de respuesta a incidentes al personal de respuesta a incidentes definido por la Repartición (identificado por nombre y/o por función).

f. Proteger el plan de respuesta a incidentes de divulgación y modificación no autorizadas.

## 3.0 CUMPLIMIENTO

Los empleados que incumplan esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y/o administrativas si correspondieren. Los no empleados, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

## 4.0 EXCEPCIONES DE POLÍTICA

Las solicitudes de excepciones a esta política serán revisadas por el Director de Ciberseguridad (DC) y Secretaría de Innovación Pública (SIP) y/o Encargado de Seguridad de la Información. Los departamentos que soliciten excepciones deberán proporcionar dichas solicitudes al DC/SIP. La solicitud debe indicar específicamente el alcance de la excepción junto con la justificación para otorgar la excepción, el posible impacto o riesgo asociado al otorgar la excepción, las medidas de mitigación de riesgos que debe tomar el Departamento de TI, iniciativas, acciones y un cronograma para lograrlo, el nivel mínimo de cumplimiento de las políticas aquí establecidas. El DC/SIP revisará dichas solicitudes; consultar con el departamento solicitante.

## 5.0 HISTORIAL DE REVISIONES

| Fecha | Descripción de Cambio | Participantes |
|---|---|---|
| 12/08/2024 | Revisión inicial | Alejandro Castro, Pablo Zalazar |
| 13/08/2024 | Visado, y corrección de errores | Alejandro Castro. |

## 6.0 REFERENCIA

Publicación especial (SP) del Instituto Nacional de Estándares y Tecnología (NIST): NIST SP 800-53a: respuesta a incidentes (IR), NIST SP 800-16, NIST SP 800-50, NIST SP 800-61, NIST SP 800-84, NIST SP 800-115

# Capítulo 28

# Política de Planificación

### 1.0 OBJETIVO

Garantizar que los recursos y sistemas de información de tecnología de la información (TI) se planifiquen con controles de seguridad efectivos y mejoras de control que reflejen las leyes, órdenes gubernamentales, directivas, regulaciones, políticas, estándares y directrices nacionales y provinciales aplicables.

### 2.0 POLÍTICA

Esta política es aplicable a todos los departamentos y usuarios de recursos y activos de TI.

1. PLAN DE SEGURIDAD DEL SISTEMA
   El Departamento de TI deberá:

   a. Desarrollar un plan de seguridad para cada sistema de información que:

      i. Sea consistente con la arquitectura gubernamental de la Repartición.

      ii. Defina explícitamente el límite de autorización para el sistema.

      iii. Describa el contexto operativo del sistema de información en términos de misiones y procesos.

      iv. Proporcione la categorización de seguridad del sistema de información, incluida la justificación de respaldo.

      v. Describa el entorno operativo para el sistema de información y las relaciones o conexiones con otros sistemas de información.

      vi. Proporcione una descripción general de los requisitos de seguridad del sistema.

      vii. Identifique cualquier superposición relevante, si corresponde.

      viii. Describa los controles de seguridad implementados o planificados para cumplir con esos requisitos, incluida una justificación de las decisiones de adaptación.

      ix. Sea revisado y aprobado por el funcionario autorizado o representante designado antes de la implementación del plan.

b. Distribuir copias del plan de seguridad y comunicar los cambios posteriores al plan al personal autorizado y/o unidades de negocio.

c. Revisar el plan de seguridad del sistema de información al menos una vez al año.

d. Actualizar el plan para abordar cambios en el sistema de información/entorno de operación o problemas identificados durante la implementación del plan o las evaluaciones de control de seguridad.

e. Proteger el plan de seguridad contra divulgación y modificación no autorizadas.

2. REGLAS DE COMPORTAMIENTO
El Departamento de TI deberá:

a. Establecer y poner a disposición de las personas que requieran acceso al sistema de información, las reglas que describen sus responsabilidades y el comportamiento esperado con respecto a la información y el uso del sistema de información.

b. Recibir un reconocimiento firmado de dichas personas, indicando que han leído, comprendido y se comprometen a respetar las reglas de conducta, antes de autorizar el acceso a la información y al sistema de información.

c. Revisar y actualizar las normas de conducta.

d. Exigir a las personas que hayan firmado una versión anterior de las reglas de conducta que lean y renuncien cuando se revisen y actualicen las reglas de conducta.

3. ARQUITECTURA DE SEGURIDAD DE LA INFORMACIÓN
El Departamento de TI deberá:

a. Desarrollar una arquitectura de seguridad para el sistema de información que:

i. Describa la filosofía general, los requisitos y el enfoque que se debe adoptar con respecto a la protección de la confidencialidad, integridad y disponibilidad de la información organizacional.
ii. Describir cómo la arquitectura de seguridad de la información se integra y respalda la arquitectura gubernamental.

iii. Describir cualquier supuesto de seguridad de la información y dependencia de servicios externos.

b. Revisar y actualizar la arquitectura de seguridad de la información al menos una vez al año, para reflejar las actualizaciones en la arquitectura gubernamental.

c. Asegurar que los cambios planificados en la arquitectura de seguridad de la información se reflejen en el plan de seguridad, las operaciones de seguridad y las compras/adquisiciones.

4. ENFOQUE DE DEFENSA EN PROFUNDIDAD
   El Departamento de TI deberá:

   a. Diseñar una arquitectura de seguridad utilizando un enfoque de defensa en profundidad que:

      i. Asigne controles de seguridad a ubicaciones definidas y capas arquitectónicas de la Repartición.

      ii. Garantizar que los controles de seguridad asignados funcionen de manera coordinada y se refuercen mutuamente.

## 3.0 CUMPLIMIENTO

Los empleados que incumplan esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y/o administrativas si correspondieren. Los no empleados, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

## 4.0 EXCEPCIONES DE POLÍTICA

Las solicitudes de excepciones a esta política serán revisadas por el Director de Ciberseguridad (DC) y Secretaría de Innovación Pública (SIP) y/o Encargado de Seguridad de la Información. Los departamentos que soliciten excepciones deberán proporcionar dichas solicitudes al DC/SIP. La solicitud debe indicar específicamente el alcance de la excepción junto con la justificación para otorgar la excepción, el posible impacto o riesgo asociado al otorgar la excepción, las medidas de mitigación de riesgos que debe tomar el Departamento de TI, iniciativas, acciones y un cronograma para lograrlo, el nivel mínimo de cumplimiento de las políticas aquí establecidas. El DC/SIP revisará dichas solicitudes; consultar con el departamento solicitante.

## 5.0 HISTORIAL DE REVISIONES

| Fecha | Descripción de Cambio | Participantes |
|---|---|---|
| 12/08/2024 | Revisión inicial | Alejandro Castro, Pablo Zalazar |
| 19/08/2024 | Visado, y corrección de errores | Alejandro Castro. |

## 6.0 REFERENCIA

Publicaciones especiales (SP) del Instituto Nacional de Estándares y Tecnología (NIST): NIST SP 800-53a – Planificación de seguridad (PL), NIST SP 800-12, SP NIST 800-18, NIST SP 800-100

# Capítulo 29

# Respuesta a Ciberincidentes

## 1.0 Propósito y Beneficios

Este estándar describe los pasos generales para responder a incidentes de seguridad informática. Además de proporcionar un flujo de proceso estandarizado, (1) identifica las partes interesadas en la **respuesta a incidentes (a partir de aquí en adelante "RI")** y establece sus funciones y responsabilidades; (2) describe las fuentes desencadenantes del incidente, los tipos de incidentes y los niveles de gravedad del incidente; y (3) incluye requisitos para pruebas anuales, actividades de lecciones aprendidas posteriores al incidente y recopilación de métricas de RI para su uso para medir la efectividad de la RI.
Los objetivos de RI, tal como se describen en este estándar, son:

- Confirmar si ocurrió un incidente;
- Proporcionar un proceso de notificación de incidentes definido;
- Promover la acumulación y documentación de información veraz;
- Establecer controles para la recuperación y el manejo adecuado de la evidencia;
- Contener el incidente y detener cualquier actividad no deseada de forma rápida y eficaz;
- Minimizar la interrupción de las operaciones de la red;
- Proporcionar informes precisos y recomendaciones útiles a la dirección; y
- Prevenir y/o mitigar la ocurrencia de futuros incidentes.

## 2.0 Declaración de información

### 2.1 Funciones y responsabilidades de las partes interesadas en RI

Para responder eficazmente a un incidente de seguridad informática, es fundamental que todas las partes interesadas de RI comprendan plenamente no sólo sus funciones y responsabilidades en el proceso de RI, sino también las funciones y responsabilidades de cada parte interesada de RI. Esto es necesario para (1) evitar la duplicación de esfuerzos; (2) minimizar las lagunas procesales que puedan ocurrir; y (3) garantizar una respuesta rápida a incidentes de seguridad informática.
Las partes interesadas en RI incluyen:

1. Responsable de seguridad de la información: El Director de Ciberseguridad (DC) asumirá la coordinación general de la RI, incluida la escalada de un incidente. El DC lidera los servicios de respuesta a incidentes para la organización.

2. Liderazgo de la entidad- Proporciona principalmente supervisión de RI, siendo su Oficial de Seguridad de la Información (ISO) o el encargado el más "práctico" en términos de actividades de gestión de RI.

3. Centro de operaciones de seguridad– El Equipo de Operaciones de Seguridad (EOS) sirve como un grupo central para la detección, análisis, seguimiento, respuesta y notificación de amenazas e incidentes cibernéticos. El EOS responde a los incidentes proporcionando RI técnico práctico y recomendará medidas para que el personal remedie y mitigue de manera que reduzca la probabilidad de futuros incidentes.

   Además, el EOS facilita la colaboración y el intercambio de información con otras Reparticiones que puedan estar experimentando incidentes iguales o similares, para ayudar a resolver el problema más rápidamente que si se hiciera por separado. El EOS recopila información sobre los tipos de vulnerabilidades que se están explotando y la frecuencia de los ataques y comparte información preventiva para ayudar a otras reparticiones a protegerse de ataques similares.
4. Primeros auxilios– Se recurrirá al personal de TI, como administradores de red, administradores de sistemas y otro personal técnico, según sea necesario, para brindar soporte y respuesta táctica al Equipo de Operaciones de Seguridad. Todo análisis forense digital debe ser realizado por el EOS o bajo su dirección.

5. Equipos de respuesta a incidentes de la Repartición– Deben estar listos equipos predefinidos que incluyan, como mínimo, personal de la Dirección o superior Autoridad, del área Legal o Asuntos Jurídicos y Responsable de Comunicaciones o Relaciones Públicas. En algunos casos, pueden verse involucrados Recursos Humanos o Personal.

6. Entidades Externas- En consulta con el Equipo de Operaciones de Seguridad, las entidades externas pueden realizar actividades prácticas de RI, como actividades de respuesta de investigación, o pueden proporcionar orientación. Por ejemplo, un proveedor de soluciones de seguridad puede brindar asistencia sobre la configuración de los dispositivos de seguridad. Las entidades externas incluyen vendedores, proveedores de servicios o autoridades encargadas de hacer cumplir la ley, incluidos, entre otros:

   - Ministerio de Seguridad nacional o provincial;
   - Fuerzas de seguridad federales o provinciales (Delitos Informáticos)
   - Proveedores de servicios de Internet
   - Proveedores de soluciones de seguridad
   - Proveedores titulares de datos

## 2.2 Flujo de RI

Este flujo de proceso de RI cubre cómo responder a situaciones específicas para que las partes interesadas de RI garanticen una respuesta efectiva y eficiente. El enfoque del proceso de RI es erradicar el problema lo más rápido posible, mientras se recopila

inteligencia procesable, para restaurar las funciones gubernamentales, mejorar la detección y evitar que vuelva a ocurrir. Una Repartición puede adoptar el flujo de proceso de RI de seis pasos como se muestra a continuación.[4]:

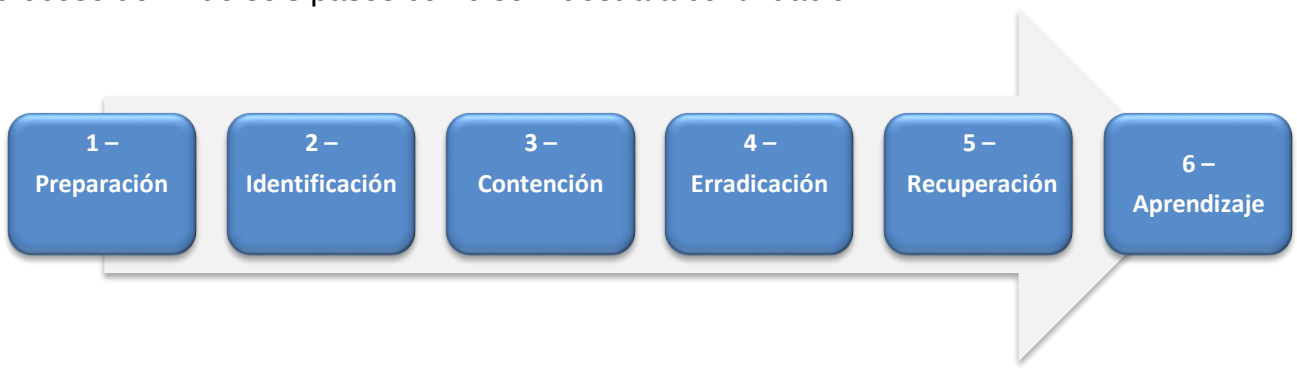


*Figura 4.1 – Flujo del proceso de respuesta a incidentes*

**Paso 1: preparación**

La planificación y preparación adecuadas para un incidente antes de que ocurra garantiza un proceso de RI más eficaz y eficiente. Las actividades asociadas con este paso incluyen el establecimiento de equipos de RI; actualizar herramientas, políticas/procedimientos y formularios/listas de verificación de RI; y garantizar que los procedimientos de comunicación de RI y las listas de contactos de las partes interesadas de RI sean precisos y estén actualizados. Una entidad debe tener una Lista de Contactos definida y actualizada y establecer múltiples canales de comunicación con todas las entidades e individuos en la Lista de Contactos de RI.

Una Repartición debe asignar la responsabilidad de un punto de contacto central para coordinar la identificación y la presentación de informes a DC. Normalmente, esto lo realiza el Encargado de seguridad designado de la Repartición. Según la Política de seguridad de la información, todos los empleados deben informar sospechas de incidentes o debilidades de seguridad de la información a la autoridad correspondiente al Encargado de seguridad designado.

El Equipo de Operaciones de Seguridad establecerá Procedimientos Operativos Estándar (SOP) para RI para reflejar los estándares y las mejores prácticas globales. Estos SOP se seguirán durante la respuesta a incidentes. Cualquier excepción debe documentarse. El Equipo de Operaciones de Seguridad debe examinar y validar periódicamente las herramientas y técnicas utilizadas para la RI. Para funcionar de manera eficiente y efectiva, el proceso de RI debe probarse periódicamente. Esto debe ocurrir al menos una vez al año. Estas pruebas se pueden lograr con capacitación sobre incidentes simulados o ejercicios prácticos utilizando escenarios realistas para proporcionar un esquema de alto nivel y un recorrido sistemático del proceso de RI y, en la medida de lo posible, deben incluir a todas las partes interesadas de RI. Estos escenarios de capacitación deben incluir 'puntos de discusión' específicos que representen oportunidades clave de aprendizaje e incorporar lecciones aprendidas, que luego puedan integrarse en el proceso de RI como parte de su revisión.

**Paso 2: Identificación**

[4]Basado en el manejo de incidentes del Instituto SANS paso a paso

La identificación implica la revisión de anomalías para determinar si ha ocurrido o no un incidente y, si ha ocurrido, determinar la naturaleza del incidente. La identificación comienza con un evento, una anomalía que se ha informado o detectado en un sistema o red. La detección se puede lograr a través de fuentes técnicas (por ejemplo, personal de operaciones, software antivirus), fuentes no técnicas (por ejemplo, informes y concientización sobre la seguridad del usuario) o ambas.

Es importante reconocer que no todos los eventos de la red o del sistema serán un incidente de seguridad. Se debe asignar un responsable para determinar si hay un incidente, clasificarlo y escalarlo según sea necesario. Normalmente, será el representante de seguridad designado por la Unidad de Organización.

Para ser eficaz en RI, los incidentes deben clasificarse y derivarse lo antes posible a las partes interesadas de RI adecuadas para promover la colaboración y el intercambio de información. La clasificación de incidentes requiere el uso de categorías de incidentes establecidas junto con una matriz de gravedad de incidentes como medio para priorizar los incidentes y determinar las actividades de RI apropiadas.

Categorías de incidentes

Es importante categorizar los incidentes comunes experimentados en toda la Repartición. Al hacerlo, las partes interesadas en RI pueden enfocar mejor sus actividades de RI. Cabe señalar que los incidentes pueden tener más de una categoría y la categorización puede cambiar a medida que se desarrolla la investigación. Una entidad puede adoptar los seis (6) US-CERT[5]categorías de incidentes de la siguiente manera:

Categorías de incidentes

| Categoría | Nombre | Descripción |
|---|---|---|
| 0 | Ejercicio/Pruebas de defensa de red | Se utiliza durante ejercicios nacionales y provinciales e internacionales y pruebas de actividad aprobadas de defensas o respuestas de redes internas/externas. |
| 1 | Acceso no autorizado | Un individuo obtiene acceso lógico o físico sin permiso a una red, sistema, aplicación, datos u otro recurso del gobierno local. |
| 2 | Denegación de servicio | Un ataque que impide o perjudica con éxito la funcionalidad normal autorizada de redes, sistemas o aplicaciones al agotar los recursos. Esta actividad incluye ser víctima o participar en la Denegación de Servicio (DoS). |
| 3 | Código malicioso | Instalación exitosa de software malicioso (p. ej., virus, gusano, caballo de Troya u otra entidad maliciosa basada en código) que infecta un sistema operativo o una aplicación. |

[5]http://www.us-cert.gov/government-users/reporting-requirements

| Categorías de incidentes | | |
|---|---|---|
| **Categoría** | **Nombre** | **Descripción** |
| 4 | Uso inadecuado | Una persona que, a sabiendas o sin saberlo, viola las políticas aceptables de uso de la informática. |
| 5 | Escaneos / Sondas / Intentos de Acceso | Incluye cualquier actividad que busque acceder o identificar la computadora de una entidad, puertos abiertos, protocolos, servicios o cualquier combinación para su posterior explotación. Esta actividad no resulta directamente en un compromiso o denegación de servicio. Los escaneos internos no autorizados se consideran incidentes. La mayoría de las exploraciones externas se consideran de rutina y, caso por caso, pueden requerir respuesta e investigación. |
| 6 | Investigación | Incidentes no confirmados que son actividades potencialmente maliciosas o anómalas que la entidad informante considera que justifican una revisión adicional. |

*Tabla 4.2 – Categorías de incidentes*

Matriz de gravedad del incidente

Todos los incidentes de seguridad de la información deben clasificarse según el nivel de gravedad para ayudar a determinar hasta qué punto se requiere una RI formal. Los niveles de gravedad se basan en el impacto gubernamental percibido del incidente. Los niveles de gravedad pueden cambiar a medida que se desarrolla la investigación. Las definiciones generales y la descripción de cada nivel de gravedad son las siguientes:

| Matriz de gravedad del incidente | | |
|---|---|---|
| **Nivel** | **Definición** | **Ejemplos** |
| Alto | Incidentes que tienen un impacto severo en las operaciones | Compromiso de datos sensibles<br>Ataque generalizado de código malicioso<br>Acceso no autorizado a sistemas críticos<br>DoS que afecta a toda la empresa |
| Medio | Incidentes que tienen un impacto significativo, o el potencial de tener un impacto severo, en las operaciones. | Ataque DoS a pequeña escala<br>Compromisos del sitio web<br>Acceso no autorizado (ataques de fuerza bruta contra FTP, ssh y otros protocolos) |
| Bajo | Incidentes que tienen un impacto mínimo con el potencial de tener un impacto significativo o grave en las operaciones. | Sondeos de red o análisis del sistema<br>Infecciones por virus aislados<br>Violaciones de uso aceptable |

*Tabla 4.3 – Matriz de gravedad del incidente*

Procedimientos de escalada

Durante un incidente, la comunicación clara y efectiva es fundamental. Como tal, un procedimiento de escalada debe abordar todas las líneas de comunicación en caso de que ocurra un incidente. Esto incluye no sólo la comunicación interna sino también la comunicación externa. La comunicación debe fluir a través de todas las partes interesadas involucradas en RI para que todos tengan la información necesaria para actuar y llevar a cabo sus responsabilidades de manera oportuna. La notificación debe realizarse lo antes posible, pero no debe retrasar que la Repartición adopte las medidas adecuadas para aislar y contener los daños.

Cada Repartición debe tener un procedimiento de escalamiento de RI que consta de (1) una matriz de escalamiento, (2) una lista de contactos actualizada con contactos alternativos y (3) múltiples canales de comunicación, todo en un esfuerzo por garantizar que la información sea apropiada y precisa se difunde rápidamente a las partes interesadas apropiadas en RI.

Alcance del incidente

El alcance inicial lo proporciona la entidad e incluye:

- Identificar objetivos potenciales (por ejemplo, sistemas comprometidos conocidos, sistemas probablemente afectados, sistemas clave);
- Definir puntos de contacto externos (por ejemplo, Internet, conexiones inalámbricas, de terceros, de acceso remoto);
- Priorizar escenarios probables (por ejemplo, amenaza interna versus externa, ataque dirigido versus objetivo de oportunidad); y
- Visualizar el entorno dentro del alcance (por ejemplo, diagrama de red, flujo de datos).

Las consideraciones para las actividades de alcance de incidentes son las siguientes:

- Confiar en fuentes de evidencia relevantes y verificadas;
- Reducir los falsos positivos y el volumen de datos;
- Evitar un alcance excesivo y un "desplazamiento del alcance"; y
- Darse cuenta de las limitaciones operativas y de recursos puede afectar el alcance.

A medida que se desarrolla información adicional relacionada con el incidente durante el proceso de RI y a medida que se involucran más partes interesadas, un incidente generalmente requiere un nuevo alcance.

Seguimiento e informes de incidentes

Un sistema de seguimiento centralizado seguro, que pueda adaptarse al acceso "necesario saber", conduce a un esfuerzo de RI más eficiente y sistemático, además de proporcionar un seguimiento de auditoría en caso de que los esfuerzos conduzcan a un procesamiento legal de la amenaza.

Como mínimo, la documentación del incidente debe contener la siguiente información:

- Fecha/hora en que se informó el incidente

- Tipo de incidente
- Fuente de notificación del incidente
- Resumen del incidente
- Estado actual del incidente.
- Todas las acciones tomadas con respecto al incidente.
- Información de contacto de todas las partes involucradas.
- Evidencia reunida durante la investigación del incidente
- Comentarios relevantes de los miembros del equipo de RI
- Próximos pasos propuestos a seguir

**Paso 3: Contención**

Este paso se centra en contener la amenaza para minimizar el daño. Es durante este paso que se recopila información para determinar cómo ocurrió el ataque. Todos los sistemas afectados dentro de la Repartición deben identificarse para que la contención (y la erradicación y recuperación) sea efectiva y completa.

La contención de incidentes implica "detener la hemorragia" y evitar que el incidente se propague. La contención se puede lograr aislando los sistemas infectados, bloqueando actividades sospechosas de la red y deshabilitando servicios, entre otras acciones. La contención varía para cada incidente dependiendo de la gravedad y el riesgo de continuar con las operaciones. El liderazgo de la Repartición toma decisiones con respecto a las medidas de contención basadas en las recomendaciones del DC y/o Responsable de Seguridad.

**Paso 4: Erradicación**

La erradicación implica eliminar elementos de la amenaza de la red gubernamental. Las medidas de erradicación específicas dependen del tipo de incidente, la cantidad de sistemas involucrados y los tipos de sistemas operativos y aplicaciones involucradas. Las medidas típicas de erradicación incluyen volver a crear imágenes de los sistemas infectados y mejorar la supervisión de la actividad del sistema.

El análisis de la información recopilada es un proceso iterativo y ocurre o vuelve a ocurrir durante las fases de contención y erradicación.

**Paso 5: Recuperación**

Una vez que se ha erradicado la causa raíz de un incidente, puede comenzar la fase de recuperación. Los objetivos de este paso son: (1) remediar cualquier vulnerabilidad que contribuya al incidente (y así prevenir incidentes futuros) y (2) recuperarse restaurando las operaciones a la normalidad. A menudo se utiliza un enfoque por fases para devolver los sistemas a su funcionamiento normal, reforzarlos para evitar futuros incidentes similares y aumentar la supervisión durante un período de tiempo adecuado. Las actividades de recuperación típicas incluyen reconstruir sistemas a partir de imágenes confiables, restaurar sistemas a partir de copias de seguridad limpias y reemplazar archivos comprometidos con versiones limpias.

Se debe tener cuidado para garantizar que los archivos restaurados desde la copia de seguridad no reintroduzcan códigos maliciosos o vulnerabilidades del incidente y que el sistema esté limpio y seguro antes de volver al uso de producción. Una vez que se

haya completado la recuperación, el líder de RI debe validar/certificar que el incidente se ha resuelto.

**Paso 6: Aprendizaje**

Un proceso de RI es tan bueno como la capacidad de ejecutarlo exitosamente. Las lecciones aprendidas pueden ser el resultado de actividades reales de RI o de pruebas de capacidad de RI, y estos resultados deben usarse para mejorar el proceso de RI identificando debilidades y deficiencias sistémicas y tomando medidas para mejorarlas. Es importante que esto tenga lugar relativamente pronto después de que se cierre el incidente.

Las lecciones aprendidas, o discusiones post mortem, proporcionan (1) un registro de los pasos tomados para responder a un ataque, (2) resultados de la investigación para determinar la causa raíz del ataque, (3) posibles mejoras a realizar, como la capacitación y certificaciones de las partes interesadas en RI, actualizaciones de procesos y procedimientos, y modificaciones técnicas. El conocimiento adquirido se puede utilizar en un esfuerzo por prevenir y/o mitigar incidentes futuros en forma de servicios proactivos. Esto puede incluir probar el proceso de RI, realizar evaluaciones de vulnerabilidad, brindar capacitación en seguridad informática, revisar políticas y procedimientos de seguridad y difundir recordatorios de seguridad cibernética.

Tanto los informes de incidentes como los resultados de estas discusiones sobre lecciones aprendidas se colocarán en una base de datos para uso futuro y se compartirán con todas las partes interesadas de RI para el conocimiento de la situación y el desarrollo profesional.

## 2.3 Métricas de respuesta a incidentes

Se deben compilar métricas de RI para cada incidente y reportarlas al DC y/o Encargado de Seguridad para el conocimiento de la situación gubernamental cuando sea posible y práctico.

Estas métricas permiten a las partes interesadas en RI (1) medir la efectividad de RI (y revelar posibles brechas) a lo largo del tiempo; (2) identificar tendencias en términos de actividades de amenaza y al hacerlo; (3) proporcionar justificación para recursos adicionales, para incluir personal, capacitación y herramientas adicionales.

| Métricas de RI | | |
|---|---|---|
| **Categoría** | **Medición** | **Descripción** |
| Incidentes | # Total de Incidentes / Año | Cantidad total de incidentes atendidos por año |
| | # Incidentes por Tipo / Año | Número total de incidentes por categoría respondidos por año |
| Tiempo | # Horas de Personal / Incidente | Cantidad total de mano de obra dedicada a resolver el incidente |
| | # Días / Incidente | Cantidad total de días dedicados a resolver el incidente |

| Métricas de RI | | |
|---|---|---|
| Categoría | Medición | Descripción |
| | # Horas de inactividad del sistema/Incidente | Total de horas de inactividad del sistema hasta que se resolvió el incidente |
| Costo | Costo monetario estimado/incidente | Costo monetario total estimado por incidente, que incluye contención, erradicación y recuperación, así como actividades de recolección y análisis (esto puede incluir costos laborales, asistencia de entidades externas, adquisición de herramientas, viajes, etc.) |
| Daño | # Sistemas afectados / Incidente | Número total de sistemas afectados por incidente |
| | # Registros comprometidos / Incidente | Número total de registros comprometidos por incidente |
| Forense | # Total de incidentes forenses apalancados / año | Número total de incidentes que requieren análisis forense (recopilación y análisis) por año |
| | # Imágenes del sistema analizadas / Incidente | Número total de imágenes del sistema analizadas por incidente |
| | # Volcados de memoria del sistema examinados/incidente | Número total de volcados de memoria física del sistema examinados por incidente |

*Tabla 4.4 – Métricas de respuesta a incidentes*

## 3.0 Cumplimiento

Los empleados que incumplan esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y/o administrativas si correspondieren. Los no empleados, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

## 4.0 Historial de revisiones

| Fecha | Descripción del cambio | Crítico |
|---|---|---|
| | | |