ANEXO A
Controles de Seguridad de la Información

CTIC-SE-P1-v.1.0

CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

1. Seguridad en recursos humanos

Es necesario establecer mecanismos de relación, en materia de seguridad de la información, entre el recurso humano y la entidad o institución pública con el objetivo de preservar la información a la que tienen acceso durante y después de la vinculación laboral.

1.1. Términos y condiciones de la relación laboral

Establecer las responsabilidades en el marco de seguridad de la información del servidor público o cualquiera que tenga un vínculo laboral con la entidad o institución pública, debe formar parte integrante de la documentación de los archivos personales de cada servidor público o cualquiera que tenga un vínculo laboral con la entidad o institución pública.

1.1.1 Acuerdo de confidencialidad

A. Objetivo

Prevenir posibles fugas, divulgación no autorizada, mal uso o resguardo de la información.

B. Aplicabilidad

Servidores públicos o cualquier persona jurídica o natural que tenga un vínculo laboral con la entidad o institución pública.

C. Directrices

i. Elaborar el acuerdo de confidencialidad.
ii. Definir las restricciones y alcances del uso de la información, así como roles y responsabilidades.
iii. Coordinar con el área jurídica o legal la legalidad del acuerdo de confidencialidad.
iv. Garantizar la anuencia del servidor público o cualquier persona natural o jurídica que tenga un vínculo laboral con la entidad o institución pública con el acuerdo de confidencialidad.
v. Revisar y actualizar el acuerdo de confidencialidad en caso de cambios sustanciales en la clasificación de la información o a requerimiento interno.
vi. Respetar los datos de carácter personal, garantizar la privacidad y protección de la información personal identificable.

1.2 Concientización, educación y formación en seguridad de la información

Se debe generar una cultura de seguridad de la información institucional que involucre a todos los servidores públicos y a cualquier persona natural o jurídica que tenga un vínculo laboral con la entidad o institución pública.

1.2.1 Capacitación y formación

A. Objetivo

Capacitar en temas relacionados a seguridad de la información.

B. Aplicabilidad

Servidores públicos o cualquier persona jurídica o natural que tenga un vínculo laboral con la entidad o institución pública.

C. Directrices

i. Realizar eventos de concientización sobre la seguridad de la información, donde además se muestren roles y responsabilidades de los funcionarios para procedimientos de seguridad.
ii. Realizar capacitaciones acerca del Plan Institucional de Seguridad de la Información y las Políticas de Seguridad de la Información incluidas, con énfasis en las áreas de desempeño de los servidores públicos a ser capacitados.
iii. Informar sobre las responsabilidades adquiridas por acción u omisión e incumplimiento al Plan Institucional de Seguridad de la Información.
iv. Informar sobre los medios y puntos de contacto en temas relacionados a seguridad de la información.
v. Evaluar el grado de conocimiento de los servidores públicos respecto al Plan institucional de Seguridad de la Información.

1.3 Sanciones o amonestaciones a consecuencia del incumplimiento del PISI institucional

Implementar mecanismos disuasivos y preventivos para los casos de incumplimiento, por acción u omisión, de los documentos normativos relacionados a seguridad de la información.

A. Objetivo

Sancionar el incumplimiento de la normativa de seguridad de la información institucional vigente.

B. Aplicabilidad

Servidores públicos y cualquier persona jurídica o natural que tenga un vínculo laboral con la entidad o institución pública.

C. Directrices

i. Establecer las sanciones al incumplimiento de la normativa de seguridad de la información institucional vigente.
ii. Verificar la concordancia de la aplicación de las sanciones a los procesos o procedimientos internos de cada entidad o institución pública.
iii. Informar sobre los alcances y consecuencias de las sanciones fruto de infracciones al PISI .

1.4 Desvinculación de personal o cambio de cargo

Es necesario velar por el resguardo de la información e intereses de la entidad o institución pública al momento de la desvinculación o cambio del cargo de algún servidor público o cualquier persona natural o jurídica que tenga un vínculo laboral.

A. Objetivo

Preservar la disponibilidad, confidencialidad e integridad de la información al momento de la desvinculación o cambio de cargo de algún servidor público.

B. Aplicabilidad

Servidores públicos y cualquier persona natural o jurídica, al término o cambio de cargo de la relación laboral.

C. Directrices

i. Elaborar un proceso y procedimiento de desvinculación del personal que considere mínimamente: la devolución de los activos de información bajo custodia, el retiro de credenciales y cuentas de acceso a servicios y sistemas que permitan precautelar la seguridad de la información.
ii. Documentar el proceso de desvinculación y cambio de cargo.
iii. Controlar las copias no autorizadas de información durante la desvinculación.
iv. Responsabilidades y deberes que serán vigentes aun después de la finalización de la relación contractual

2. Gestión de activos de información

Con el fin de preservar la integridad, disponibilidad y confidencialidad de los activos de información, se debe administrar, controlar y asignar responsabilidades en el uso y protección de los mismos.

2.1. Identificación y responsables de los activos de información

Identificar los activos de información de la entidad o institución pública y definir las responsabilidades para una protección apropiada.

2.1.1. Inventario de activos de información

A. Objetivo

Inventariar todos los activos de información dentro de los alcances del Plan Institucional de Seguridad de la Información.

B. Aplicabilidad

Activos de información de la entidad o institución pública.

C. Directrices

i. Identificar los activos de información considerando mínimamente: el tipo de activo, el formato, la ubicación, la información de soporte, la información sobre licencias y el valor para la entidad o institución pública.
ii. Clasificar los activos de información.
iii. Asignar un valor cuantitativo y/o cualitativo a cada uno de los activos.
iv. Revisar y actualizar el inventario de activos de información mínimamente una vez al año y/o cuando se requiera.
v. Restringir el acceso al inventario solo al personal autorizado de la entidad o institución pública.
vi. El inventario podrá incluir en caso de no ser tangible el ciclo de vida de la información donde se considere la creación, procesamiento, almacenamiento, transmisión, eliminación y destrucción.

2.1.2. Responsabilidad y custodia de los activos de información

A. Objetivo

Asignar para cada activo de información un responsable y/o custodio de acuerdo a sus funciones y competencias.

B. Aplicabilidad

Responsables/custodios de los activos de información.

C. Directrices

i. Identificar a los responsables y/o custodios de activos de información.
ii. Documentar el proceso de asignación y devolución de los activos de información a propietarios y/o custodios.
iii. El responsable identificado en caso de no ser una persona, puede ser una entidad que cuente con las responsabilidades de la dirección aprobada para controlar todo o parte del ciclo de vida de la información, también el propietario puede no tener los derechos de propiedad del activo, pero sí de custodia.

2.1.3. Uso aceptable de los activos de información

A. Objetivo

Establecer las restricciones y condiciones de uso adecuado de activos de información.

B. Aplicabilidad

Responsables y/o custodios de activos de información.

C. Directrices

i. Definir los requisitos de seguridad en relación a los activos de información.
ii. Establecer reglas para el uso correcto de los activos de información dentro y fuera de las instalaciones.
iii. Elaborar e implementar un reglamento de uso aceptable de activos de información, considerando mínimamente los puntos anteriores.
iv. Garantizar la aceptación de las restricciones y condiciones de uso de los activos de información a todos los servidores públicos y cualquier persona natural o jurídica que tenga un vínculo contractual con la entidad o institución pública, a los cuales se les haya asignado uno de ellos.

2.1.4. Devolución de los activos de información

A. Objetivo

Precautelar la disponibilidad, integridad y confidencialidad de los activos de información al momento de la desvinculación o cambio de cargo.

B. Aplicabilidad

En casos de desvinculación o cambio de cargos.

C. Directrices

i. Desarrollar e implementar un procedimiento de devolución de activos de información.
ii. En los casos donde el empleado o el usuario externo cuente con conocimiento importante para las operaciones de continuidad de

la institución, dicha información se debería documentar y transferir.

2.2. Clasificación de la información

Identificar y clasificar la información según el grado de sensibilidad y criticidad para su uso y tratamiento adecuado.

2.2.1. Clasificación

A. Objetivo

Identificar y clasificar la información en relación a su valor, requisitos legales, sensibilidad, criticidad para su uso y tratamiento adecuado en la entidad o institución pública.

B. Aplicabilidad

Información, en cualquier medio en el que se encuentre.

C. Directrices

i. Elaborar un procedimiento de clasificación de la información institucional, que contenga los requisitos, nivel de clasificación, los responsables, las restricciones y la gestión de la información en general.
ii. Establecer requisitos de protección para cada nivel de clasificación definido que deberán considerar las necesidades de la entidad o institución pública respecto a la apertura o restricción de la información.
iii. Reclasificación de la información de acuerdo a requerimiento y/o normativa vigente.

2.2.2. Etiquetado y manejo

A. Objetivo

Manejar adecuadamente la información, acorde a los requisitos y nivel de clasificación establecidos.

B. Aplicabilidad

Información, en cualquier medio en el que se encuentre.

C. Directrices

i. Definir dentro del procedimiento de clasificación institucional el proceso de etiquetado de la información en formatos físicos y digitales.
ii. Adecuación del proceso de etiquetado a los niveles de sensibilidad y criticidad establecidos.
iii. Definir los procedimientos de manejo, procesamiento, almacenamiento, transmisión, desclasificación y destrucción segura de la información, para cada nivel de clasificación.

2.2.3. Protección del archivo

A. Objetivo

Gestionar la seguridad del archivo de documentos.

B. Aplicabilidad

Documentación archivada.

C. Directrices

i. Definir un proceso y/o procedimiento para el archivo de documentación

institucional.

ii. Elaborar controles para evitar la modificación y el acceso no autorizado a la información archivada.

iii. Elaborar controles para el acceso al archivo.

iv. Elaborar procedimientos de solicitud de documentación archivada.

v. Elaborar controles para la trazabilidad de la documentación archivada, que permita revisar las modificaciones realizadas

2.3. Gestión de medios de almacenamiento removibles

La gestión de medios de almacenamiento removibles es necesaria para evitar la divulgación, modificación, manipulación o destrucción de información no autorizada en los medios de almacenamiento.

2.3.1. Gestión de medios removibles

A. Objetivo

Gestionar los medios informáticos removibles de acuerdo a los niveles de clasificación de información de la entidad o institución pública.

B. Aplicabilidad

Información en medios removibles.

C. Directrices

i. Elaborar procedimientos de uso de medios removibles donde mínimamente se establezcan quién, cómo, cuándo y para qué se accede a esos medios.

ii. Elaborar e implementar procesos y/o procedimientos para la autorización, uso y retiro de medios removibles al interior y exterior de la entidad o institución pública.

iii. Mantener un registro de auditoría del uso de medios removibles.

iv. Considerar el uso de cifrado de información en medios removibles, de acuerdo a la clasificación de información.

v. El contenido de los medios removibles que ya no se requieran deben ser destruidos e irrecuperables.

2.3.2. Eliminación segura de información

A. Objetivo

Eliminar la información de manera segura independientemente del medio en el que se encuentre, de acuerdo a los niveles de clasificación definidos por la entidad o institución pública.

B. Aplicabilidad

Información, en cualquier medio en el que se encuentre.

C. Directrices

i. Establecer y elaborar procesos/procedimientos para la eliminación de información, independientemente del medio en el que se encuentre, de acuerdo a los niveles de clasificación definidos por la entidad o institución pública y normativa legal vigente en el Estado Plurinacional de Bolivia.

ii. Para la eliminación de información, considerar la normativa legal vigente relacionada a la retención y resguardo de información.

2.3.3. Traslado físico de los medios de almacenamiento

A. Objetivo

Proteger los medios de almacenamiento que contienen información contra el acceso, uso y manipulación no autorizada al interior y fuera de las instalaciones de la entidad o institución pública.

B. Aplicación

Medios de almacenamiento.

C. Directrices

i. Elaborar procesos/procedimientos para el traslado de medios de almacenamiento.
ii. Establecer controles de protección física en medios de almacenamiento que eviten la intercepción, copia, modificación y destrucción.
iii. Mantener un registro de los medios de almacenamiento que permita identificar el contenido y custodio.
iv. En caso de considerar como no necesaria la información almacenada en cualquier medio removible, la misma será retirada de la entidad o institución pública sin posibilidad de recuperación.

3. Control de accesos

Gestionar los accesos a servicios y aplicaciones que permitan controlar, autorizar y asignar privilegios a cuentas de usuario.

3.1. Documentos normativos y operativos para el control de accesos

Establecer e implementar el reglamento para el control de accesos.

3.1.1. Normativa de control de acceso

A. Objetivo

Prevenir el acceso no autorizado a servicios, sistemas y aplicaciones.

B. Aplicabilidad

Aplica a sistemas, servicios y aplicativos de los que hace uso la entidad o institución pública para el cumplimiento de sus funciones.

C. Directrices

i. Elaborar un reglamento de control de accesos.
ii. El reglamento deberá establecer el objetivo, alcance, roles, frecuencias y responsabilidades para el control de accesos.
iii. El reglamento deberá ser revisado y actualizado cada cierto periodo de tiempo según normativa interna de la entidad o a la ocurrencia de un cambio significativo.
iv. Establecer sanciones al incumplimiento e infracciones en el control de accesos.

v. Implementar registros de acceso acorde a las necesidades de la entidad o institución pública.
vi. Se deberá establecer la periodicidad de cambios de información de autenticación.
vii. Establecer en las reglas la premisa “Generalmente todo está prohibido a menos que se permita de forma expresa”.

3.2. Administración de accesos

Administrar la creación, registro y cancelación de cuentas de acceso para usuarios y las responsabilidades de uso adecuado de la información de autenticación, de parte de los usuarios.

3.2.1. Administración de accesos, cancelación y privilegios de usuarios

A. Objetivo

Gestionar la creación y cancelación de cuentas de usuario para los distintos servicios, sistemas y aplicaciones que dispone la entidad o institución pública.

B. Aplicabilidad

Accesos a servicios, sistemas y aplicaciones.

C. Directrices

i. Se deberán establecer los requisitos de autorización para la creación y asignación de roles y privilegios de una cuenta.
ii. Se deberán establecer procesos/procedimientos que reflejen el flujo de actividades a seguir, responsables, tiempos, quién autoriza, quién es consultado, quién es informado, quién es responsable de la cuenta de acceso y la forma y medio de entrega de las credenciales. Se deberá tomar en cuenta el criterio de menor privilegio.
iii. Se deberá establecer el flujo de actividades a seguir para la revisión y cancelación de accesos al momento de la desvinculación laboral.
iv. Identificar de forma única el acceso de los usuarios. Para esto se recomienda utilizar servicios de autenticación centralizada.
v. Elaborar procesos/procedimientos especiales para el acceso a servicios privilegiados como bases de datos, sistemas operativos y aplicaciones de administración.
vi. Para accesos privilegiados se deberán implementar medidas de seguridad adicionales que permitan monitorear y verificar las actividades acorde a las funciones establecidas.
vii. Las cuentas de acceso temporal o de invitados deberán contar con la autorización correspondiente.
viii. Habilitar las cuentas de acceso basado en roles de usuario para el procesamiento, administración, consulta o uso de la información.
ix. Establecer el periodo de tiempo de inactividad máximo que deshabilite las cuentas de acceso.
x. Establecer procesos/procedimientos para gestionar credenciales de cuentas perdidas, robadas o comprometidas.
xi. Implementar técnicas seguras para fortalecer la información de autenticación.

3.2.2. Responsabilidades de los usuarios para la autenticación

A. Objetivo

Asegurar que la información de autenticación tenga un uso responsable acorde al reglamento de acceso.

B. Aplicabilidad

Usuarios que cuenten con credenciales de acceso a sistemas, servicios y aplicaciones.

C. Directrices

i. Capacitar y concientizar sobre las responsabilidades del uso de credenciales de acceso.
ii. Se deberá dejar constancia sobre la aceptación del servidor público para el uso responsable de la información de accesos.
iii. Los servidores públicos deben evitar mantener la información de autenticación en lugares visibles o de acceso fácil para los demás.
iv. Los usuarios deberán cumplir el cambio de contraseñas de acuerdo a la periodicidad y requisitos de seguridad que se establezca en la normativa de control de accesos.
v. La información de autenticación no deberá compartirse sin previa autorización justificada.
vi. La información de autenticación no deberá utilizarse para otros fines ajenos a la funciones asignadas de la entidad o institución pública.
vii. El usuario propietario de la cuenta de acceso es responsable del uso de la contraseña.

3.2.3. Revisión, eliminación o ajuste de los derechos de acceso

A. Objetivo

Revisar, eliminar o ajustar los derechos de acceso a servicios, sistemas y aplicaciones.

B. Aplicabilidad

Cuentas de acceso.

C. Directrices

i. Revisar periódicamente los derechos de acceso para identificar accesos no autorizados.
ii. Se deberán revisar los accesos privilegiados con más frecuencia y renovar los mismos en intervalos de tiempo razonables.
iii. Mantener un registro de las modificaciones de privilegios.

3.3. Control de acceso a redes y servicios de red

Gestionar el acceso a las redes de datos de la entidad o institución pública para prevenir accesos no autorizados y riesgos. La entidad debe establecer parámetros mínimos de cifrado para proteger la confidencialidad e integridad de la información.

3.3.1. Acceso remoto

A. Objetivo

Establecer un proceso/procedimiento para la gestión de acceso remoto a servicios, sistemas y aplicaciones.

B. Aplicabilidad

Solicitudes de acceso remoto.

C. Directrices

i. Establecer requisitos técnicos mínimos para la identificación y autenticación de usuarios para una conexión remota.
ii. Se deberá exigir la autorización por parte del propietario de la información.
iii. La entidad deberá definir la información que puede ser accedida y administrada mediante esta conexión, tomando en cuenta la clasificación de la información.
iv. Monitorear los accesos remotos a servicios, sistemas y aplicaciones.
v. Implementar controles de acceso a los servicios de red o aplicaciones de acuerdo a requisitos de autorización y privilegios de uso.
vi. Previsión de procedimientos de respaldo de continuidad del negocio en caso de fallas en los accesos remotos.

3.3.2. Acceso por redes inalámbricas

A. Objetivo

Gestionar la solicitud de accesos a redes inalámbricas de la Institución.

B. Aplicabilidad

Solicitudes de acceso a redes inalámbricas.

C. Directrices

i. Elaborar y establecer un proceso/procedimiento para la gestión de acceso a redes inalámbricas.
ii. Establecer requisitos técnicos mínimos para la identificación y autenticación de usuarios.
iii. La entidad deberá definir la información a la que se puede acceder mediante esta conexión.
iv. Monitorear los accesos de la red inalámbrica.
v. Implementar protección de las redes inalámbricas para evitar accesos no autorizados, en lo posible utilizando técnicas criptográficas.

3.3.3. Acceso de dispositivos móviles

A. Objetivo

Definir restricciones técnicas y uso de la información accedida a través de teléfonos inteligentes o dispositivos móviles para proteger la integridad y confidencialidad de la información.

B. Aplicabilidad

Acceso mediante teléfonos inteligentes, dispositivos móviles.

C. Directrices

i. Establecer requisitos técnicos mínimos para la identificación y autenticación de usuarios de acceso desde teléfonos inteligentes y dispositivos móviles.
ii. La entidad o institución debe definir la información que puede ser accedida mediante estos dispositivos.
iii. Se debe monitorear los accesos.

4. Criptografía

El uso de técnicas criptográficas aporta mayores niveles de seguridad para proteger la confidencialidad, autenticidad e integridad de la información, además del no repudio y autenticación.

4.1. Controles criptográficos

Utilizar técnicas criptográficas para proteger la confidencialidad, autenticidad e integridad de la información.

4.1.1. Uso de criptografía

A. Objetivo

Preservar la confidencialidad, autenticidad e integridad de la información, además del no repudio y autenticación.

B. Aplicabilidad

Información de acuerdo a los niveles de clasificación establecida e información transmitida a través de redes de comunicación.

C. Directrices

i. Elaborar e implementar un reglamento sobre el uso de criptografía para la protección de la información.
ii. Definir la fortaleza y la calidad del algoritmo de cifrado de acuerdo al tipo y criticidad de la información.
iii. Utilizar cifrado para proteger la información en medios de almacenamiento, transferencia de archivos, información transmitida por redes de comunicación y otros que se considere necesario.
iv. Utilizar firma digital para asegurar la autenticidad e integridad de la información.
v. Elaborar un proceso/procedimiento para la administración de claves, que considere: la generación, distribución, almacenamiento, cambio o actualización, recuperación, respaldo, destrucción y otras que se considere necesario.
vi. Utilizar técnicas criptográficas de claves bajo custodia.

5. Seguridad física y ambiental

Asegurar áreas e instalaciones donde se genere, procese, transmita o almacene información considerada sensible y critica para la entidad o institución pública, con el objetivo de prevenir accesos no autorizados que comprometan la seguridad de la información.

5.1. Áreas e instalaciones seguras

Establecer medidas de seguridad física en áreas e instalaciones denominadas seguras o criticas de la entidad o institución pública.

5.1.1. Seguridad física en áreas e instalaciones

A. Objetivo

Prevenir y controlar el acceso físico no autorizado a instalaciones seguras o críticas de la entidad o institución pública.

B. Aplicabilidad

Áreas e instalaciones denominadas seguras donde se genere, procese, almacene o transmita información considerada sensible y crítica.

C. Directrices

i. Elaborar un reglamento de control de acceso físico.
ii. El reglamento debe considerar la identificación de áreas e instalaciones seguras o críticas, requisitos de seguridad para el ingreso de personal autorizado, condiciones de trabajo y operación.
iii. Identificar las áreas e instalaciones consideradas seguras o críticas.
iv. Elaborar procesos/procedimientos de acceso a las diferentes áreas e instalaciones según las características de seguridad de la información.
v. El acceso a áreas e instalaciones deberá ser autorizado.
vi. Señalizar las áreas e instalaciones denominadas seguras.
vii. Contar con áreas de recepción para el control y autorización de ingreso a las instalaciones de la entidad o institución pública.
viii. Instalar sistemas de monitoreo y vigilancia enmarcados a la normativa legal vigente.
ix. Contar con procesos/procedimientos para la entrega de grabaciones de sistemas de monitoreo y vigilancia de la entidad o institución pública.
x. Se deberá contar con equipamiento para mitigar posibles incendios, los cuales deben ser normados, revisados y probados periódicamente.
xi. Los ingresos y salidas de visitas deberán ser registradas, autorizadas y controladas. Asimismo deberán portar la identificación de visitante en lugar visible.
xii. Los servidores públicos deberán portar la identificación correspondiente en un lugar visible.
xiii. La seguridad física perimetral de la entidad o institución pública deberá inspeccionar y verificar el ingreso de elementos que comprometa la seguridad.
xiv. Implementar mecanismos de alerta al interior y exterior de las instalaciones ante la ocurrencia de eventos de seguridad.
xv. Se deberán realizar simulacros de evacuación y respuesta ante amenazas internas, externas, ambientales y/o revueltas sociales.

xvi. Impedir el acceso a las instalaciones a personas no autorizadas que no tienen relación directa o indirecta con las funciones de la entidad o institución pública.
xvii. Contar con señalética visible, para evacuaciones o contingencias de la institución.

5.1.2. Trabajo en áreas e instalaciones seguras

A. Objetivo

Gestionar las actividades de trabajo y operación dentro de las áreas e instalaciones acorde a los requisitos de seguridad.

B. Aplicabilidad

Aplicable a áreas e instalaciones seguras.

C. Directrices

i. Se deberán definir las acciones permitidas y no permitidas en las áreas o instalaciones consideradas seguras.
ii. En instalaciones con información sensible se deberá evitar el trabajo no supervisado a servidores públicos y terceras personas para evitar posibles incidentes de seguridad.
iii. El uso de cámaras de seguridad y otros controles deberán estar sujetos a normativa legal, que autorice el uso de las mismas en instalaciones donde se trabaje.
iv. El personal que trabaje en estas áreas deberá estar al tanto de las acciones permitidas y no permitidas y firmar un documento de aceptación de las mismas.

5.2. Equipamiento

Proteger el equipamiento interno y externo de la entidad o institución pública para prevenir el robo, daño, pérdida o compromiso de los mismos.

5.2.1. Seguridad del equipamiento

A. Objetivo

Prevenir y/o minimizar el impacto sobre el equipamiento ante amenazas, peligros ambientales y accesos no autorizados.

B. Aplicabilidad

Equipamiento interno y externo de la entidad o institución pública.

C. Directrices

i. Los servidores públicos deberán conocer los cuidados de seguridad en el uso del equipamiento.
ii. Las instalaciones con información y equipamiento crítico para las operaciones de la entidad deberán ser controladas para evitar el acceso no autorizado y su compromiso.
iii. Implementar controles para minimizar el impacto ocasionado por condiciones ambientales, incendios, inundaciones, polvo, vibraciones, interferencias eléctricas y otros.
iv. Establecer criterios para restringir el consumo de alimentos en proximidades de áreas e instalaciones seguras.

v. Realizar mantenimientos periódicos y pruebas de funcionalidad por personal calificado al equipamiento de acuerdo a las especificaciones del fabricante.
vi. Mantener y documentar los registros de fallas de operación del equipamiento, mantenimientos preventivos y correctivos.
vii. Se deberá llevar un inventario de las especificaciones técnicas de los equipos adquiridos.
viii. Los equipos, la información y el software no se deberán retirar de las instalaciones sin previa autorización, para ello se debe establecer responsables y responsabilidades.
ix. Se deberá respaldar la información que contiene el equipo previo a la destrucción de la misma.

5.2.2. Escritorio y pantalla limpia

A. Objetivo

Minimizar el riesgo de acceso no autorizado para prevenir la divulgación, uso indebido, robo de información o modificación.

B. Aplicabilidad

Información considerada sensible y crítica.

C. Directrices

i. La información sensible y crítica en medios de almacenamiento físico deben ser resguardados bajo llave u otro mecanismo de control.
ii. Bloquear la pantalla cuando se encuentre sin supervisión.
iii. Finalizar sesiones activas en aplicaciones o servicios de redes cuando no sean utilizadas
iv. Se deberán controlar los medios de almacenamiento conectados al equipo.
v. En instalaciones de atención al público se deberá mantener el escritorio despejado.
vi. Se deberá mantener un monitoreo continuo para el cumplimento de escritorio y pantalla limpia.

5.3. Seguridad física y ambiental en el centro de procesamiento de datos

Establecer controles de seguridad físico ambiental para la operación del Centro de Procesamiento de Datos – CPD.

5.3.1. Condiciones operativas

A. Objetivo

Garantizar las condiciones operativas del centro de procesamiento de datos.

B. Aplicabilidad

Centro de procesamiento de datos.

C. Directrices

i. Establecer procesos/procedimientos formales para la administración del CPD, en cuanto a accesos, mantenimiento de equipos, supervisión de trabajos externos y otros no limitativos a la presente directriz.

ii. La instalación física del CPD deberá contar con medidas de seguridad que eviten el acceso no autorizado, la debida separación de otros ambientes que comprometan la operación normal del CPD.
iii. Implementar medidas de seguridad ambiental para minimizar riesgos de incendio, inundación, polvo, humedad, vibraciones, interferencia de suministro de energía, interferencia de las comunicaciones y radiación electromagnética.
iv. En función de los requisitos de seguridad que se establezcan, se deberán implementar controles de autenticación robustos para el acceso al CPD.
v. El acceso físico a terceros deberá contar con autorización formal y escrita para trabajos al interior del CPD bajo supervisión.
vi. La disposición del equipamiento al interior del CPD debe estar organizado y distribuido.
vii. Se debe elaborar un mapa de la disposición del equipamiento del CPD.
viii. Las condiciones de operación del equipamiento deberán estar bajo especificaciones del fabricante.
ix. Se debe controlar la temperatura de operación del CPD.
x. Se deberá implementar dispositivos de enfriamiento y extracción de aire.
xi. El CPD deberá estar debidamente señalizado e iluminado.
xii. Se deberá instalar alarmas de detección de fallas en el suministro eléctrico y condiciones ambientales.
xiii. Se deberá organizar el cableado al interior del CPD, en lo posible cumplir con un cableado estructurado.
xiv. El suministro eléctrico al equipamiento del CPD deberá estar regulado y cumplir con las especificaciones técnicas.
xv. De acuerdo a requerimientos de disponibilidad, se deberá implementar suministro alterno de energía eléctrica y/o banco de baterías.
xvi. Se deberán programar mantenimientos periódicos del equipamiento del CPD.

6. Seguridad de las operaciones

Garantizar y asegurar que las actividades operacionales en instalaciones de procesamiento de información se realicen de forma correcta.

6.1. Responsabilidad de las operaciones

Establecer responsables y responsabilidades para la ejecución de operaciones.

6.1.1. Documentación de procedimientos operacionales

A. Objetivo

Documentar y esquematizar procedimientos de operación.

B. Aplicabilidad

Actividades operativas en instalaciones de procesamiento de información.

C. Directrices

i. Identificar los procesos operacionales relacionados a seguridad de la información que requieran ser formalizados y documentados.
ii. Elaborar procesos/procedimientos que describan los procesos operacionales mediante esquemas (flujogramas) explicados en un lenguaje de fácil entendimiento.
iii. Los procedimientos deberán ser comunicados y estar a disposición de los servidores públicos que así lo requieran.
iv. Se deberá documentar la instalación, configuración, recuperación, reinicio y mantenimiento de Infraestructura Tecnológica.

6.1.2. Gestión de cambios

A. Objetivo

Controlar y documentar cambios significativos en las operaciones.

B. Aplicabilidad

Procesos estratégicos e instalaciones y tecnologías de la información.

C. Directrices

i. Designar responsables para la aprobación de cambios.
ii. Identificar y registrar cambios significativos en procesos operativos.
iii. Los cambios de configuración deberán considerar el impacto asociado y realizarse en un ambiente controlado.
iv. Elaborar procesos/procedimientos para realizar un retroceso y/o abortar los cambios ante errores o eventos inesperados y para la recuperación ante cambios fallidos o imprevistos
v. Comunicar de forma previa y posterior a los interesados sobre los cambios autorizados a realizarse.

6.1.3. Gestión de la capacidad

A. Objetivo

Adaptar, supervisar el uso de recursos críticos y proyectar futuros requisitos para asegurar el desempeño, disponibilidad y un uso eficiente de los mismos.

B. Aplicabilidad

Aplicable a tecnologías de la información y cualquier otro recurso denominado crítico.

C. Directrices

i. Identificar los recursos críticos e indispensables para las operaciones.
ii. Se deberán revisar y eliminar los datos obsoletos almacenados.
iii. Se deberá sacar de servicio a las aplicaciones, sistemas, bases de datos o entornos en desuso y/o obsoletos.

6.2. Respaldos.

Brindar protección contra la pérdida de datos y generar respaldos de la información.

6.2.1. Respaldos de información

A. Objetivo

Preservar la disponibilidad de la información.

B. Aplicabilidad

Información sensible y/o crítica.

C. Directrices

i. Identificar la información estratégica y clave para el cumplimiento de los objetivos institucionales.

ii. Se deberán establecer procesos y/o procedimientos de respaldo, donde se brinden los requisitos institucionales para realizar copias de respaldo, la periodicidad, pruebas de restauración, tiempos de retención de los respaldos en función a los requisitos institucionales y la normativa nacional.

iii. Se deberán respaldar y restaurar la información y configuración de redes, bases de datos, servicios, servidores, servidores virtuales entre otros.

iv. Se deberán establecer frecuencias de respaldos de acuerdo a los requisitos de seguridad y/o criticidad de la información de la entidad o institución pública.

v. Se deberá extraer sumas de comprobación a copias de respaldo para preservar la integridad de la información y en caso de ser necesario se deberá cifrar la información para mantener la integridad de la misma.

vi. Se deberán realizar regularmente pruebas de restauración a los respaldos para verificar su operatividad.

vii. El ambiente para el almacenamiento de copias de respaldo deberán contar con las condiciones ambientales adecuadas.

viii. En caso de tratarse de información crítica y/o estratégica se deberán almacenar los respaldos en múltiples medios de acuerdo a requerimiento.

ix. En situaciones donde el respaldo contenga información confidencial, estas deben estar protegidas con el uso de técnicas criptográficas.

7. Seguridad de las comunicaciones

Establecer controles que permitan proteger la información transmitida a través de las redes de telecomunicaciones reflejada en documentos.

7.1. Gestión de la seguridad en redes

Garantizar la protección y la disponibilidad de la Información en las redes de datos.

7.1.1. Gestión de la red

A. Objetivo

Gestionar y administrar las redes de datos y la información en tránsito por este medio.

B. Aplicabilidad

Redes de datos.

C. Directrices

i. Establecer un reglamento para la gestión de la red.
ii. El reglamento debe considerar roles y responsabilidades, procedimientos, requisitos de seguridad, tipos, métodos de autenticación, monitoreo, autorización para acceso acorde al control de accesos y administración de la infraestructura de red.
iii. Considerar la implementación de dispositivos de red redundantes para puntos de fallo único donde la disponibilidad sea un factor crítico.
iv. Elaborar procesos/procedimientos para la gestión de la infraestructura de red.
v. Implementar controles para el resguardo de la integridad, confidencialidad, disponibilidad, no repudio y trazabilidad de la información transmitida al interior y exterior de la entidad o institución pública.
vi. El cableado de red a nivel de núcleo, distribución y acceso deberá estar identificado, etiquetado y ser operativo.
vii. Se deberán elaborar y actualizar periódicamente los diagramas de red y documentar la arquitectura de la red.
viii. Establecer las condiciones de uso aceptable de internet, considerando restricciones para la conexión a internet, siguiendo el principio del mínimo privilegio que garantice la calidad de servicio.
ix. Restringir el ancho de banda para recursos de alto consumo acorde al puesto laboral.

7.1.2. Seguridad en servicios de red

A. Objetivo

Establecer mecanismos de seguridad para la gestión y uso de servicios de red internos y externos.

B. Aplicabilidad

Servicios de red internos y externos.

C. Directrices

i. Implementar controles de conexión, autenticación y cifrado para los servicios de red.
ii. En función de las necesidades de protección de confidencialidad de la información, considerar la implementación de controles para la comunicación segura en servicios de red.
iii. Se recomienda que servicios de red externos se encuentren en una o varias zonas desmilitarizadas.

7.1.3. Seguridad en la red perimetral

A. Objetivo

Proteger la infraestructura de red interna ante amenazas que se originan de redes ajenas y/o públicas.

B. Aplicabilidad

Infraestructura de red.

C. Directrices

i. Implementar controles de seguridad perimetral que protejan la red ante posibles intrusiones.
ii. De acuerdo a los requisitos de seguridad se deberán implementar y documentar reglas de acceso y salida en los dispositivos de seguridad.
iii. Establecer una o varias zonas desmilitarizadas (DMZ).
iv. Se deberán implementar reglas de control de salida y registro según corresponda.
v. Se deberá monitorear regularmente la actividad en las redes de datos.
vi. Se deberán implementar protocolos de conexión segura.
vii. Se deberán implementar, cuando se vea necesario, parámetros técnicos de encriptación para conexiones seguras y reglas de seguridad.

7.1.4. Segmentación de la red

A. Objetivo

Separar la red en subredes de acuerdo a requerimiento institucional.

B. Aplicabilidad

Red institucional, sistemas, servicios, bases de datos, servidores y grupos de usuarios entre otros.

C. Directrices

i. Segmentar la red para los sistemas, servicios informáticos, bases de datos, servidores y grupos de usuarios entre otros.
ii. Para un uso más eficiente de las redes de datos se recomienda utilizar redes locales virtuales (VLAN).
iii. Las regionales deberán tener un subdominio de red específico.
iv. Segmentar las salidas de internet relacionadas con el consumo interno de servicios.
v. Se deberá segmentar el dominio institucional interno (DNS interno) del dominio institucional externo (DNS externo).
vi. Se deberá establecer una o varias zonas desmilitarizadas (DMZ) de acuerdo a requerimiento.

7.1.5. Seguridad en redes WIFI

A. Objetivos

Gestionar la seguridad de redes WI FI.

B. Aplicabilidad

Redes WI FI.

C. Directrices

i. Comunicar e informar las redes WI FI oficiales y autorizadas para uso.
ii. Concientizar sobre el uso seguro de las redes WI FI, que informe sobre los riesgos de conexión a redes desconocidas y no autorizadas.

iii. Implementar una red virtual local dedicada para redes WI FI diferente a la red cableada.
iv. Filtrar el acceso a la red WI FI por dirección MAC, servidor proxy o cualquier otro método de acuerdo al reglamente de gestión de la red de comunicaciones.
v. Utilizar algoritmos de cifrado robustos en las redes WI FI.

7.2. Seguridad del servicio de mensajería electrónica

Gestionar de forma eficiente y segura el servicio de mensajería y/o correo electrónico.

7.2.1. Mensajería y correo electrónico

A. Objetivo

Asegurar la disponibilidad, integridad y confidencialidad de la información transmitida a través de estos servicios.

B. Aplicabilidad

Mensajería y correo electrónico institucional.

C. Directrices

i. Elaborar un reglamento de uso aceptable del correo electrónico institucional.
ii. El reglamento debe establecer reglas de uso del servicio de correo electrónico y mensajería.
iii. El servicio de correo electrónico deberá ser independiente y pertenecer a un dominio institucional, evitando el uso de correos comerciales.
iv. El servicio de correo electrónico deberá implementarse en un servidor independiente.
v. Utilizar técnicas de autenticación robustas, además de control a las redes de acceso público.
vi. Las cuentas de usuario deberán ser autenticadas para prevenir y controlar la suplantación de correo electrónico.
vii. Utilizar protocolos y puertos seguros para la configuración del servicio de correo electrónico.
viii. Gestionar regularmente el almacenamiento de correo electrónico basura.
ix. Se deberán establecer la restricción de uso para archivos adjuntos.
x. Se deberá instalar software anti-spam.

7.3. Control sobre información transferida

Asegurar la información transferida.

7.3.1. Transferencia de información

A. Objetivo

Preservar la integridad y confidencialidad de la información transferida.

B. Aplicabilidad

Información institucional transferida.

C. Directrices

i. Definir los requisitos de seguridad para la transferencia de información de acuerdo a la criticidad y sensibilidad de la misma.
ii. Elaborar procesos/procedimientos orientados a prevenir la interceptación, manipulación, duplicación, repetición, descubrimiento no autorizado y destrucción de la información transferida en cualquier medio.
iii. Utilizar técnicas de cifrado para transferencia de información sensible y crítica.
iv. Se deberá firmar un acuerdo de confidencialidad para la transferencia de la información entre partes, de acuerdo a la criticidad y sensibilidad de la misma.

8. Desarrollo, mantenimiento y adquisición de sistemas

Establecer requisitos de seguridad para el desarrollo, mantenimiento y adquisición de sistemas que consideren pruebas de seguridad, pruebas de calidad y aceptación para desarrollos internos y externos.

8.1. Desarrollo y mantenimiento de sistemas

Establecer requisitos de seguridad para el diseño, desarrollo, pruebas y mantenimiento de sistemas nuevos o existentes.

8.1.1. Elaboración de la normativa de desarrollo

A. Objetivo

Normar el desarrollo y mantenimiento seguro de sistemas.

B. Aplicabilidad

Desarrollo y mantenimiento de sistemas nuevos y existentes.

C. Directrices

i. Elaborar un reglamento que considere los requisitos de seguridad, roles y responsabilidades para el desarrollo y mantenimiento de sistemas apoyado en procesos/procedimientos.
ii. El reglamento debe ser revisable, actualizable y comunicado a las partes interesadas.
iii. Elaborar procesos/procedimientos para el control de versiones, despliegues, pruebas de seguridad, evaluación de vulnerabilidades, codificación segura, nuevos parches, correcciones y otros no limitativos a la presente directriz.
iv. Realizar procesos de gestión de actualizaciones de sistemas en caso de ser necesario. Todos los cambios deben ser probados, validados, evaluados, documentados y comunicados previamente.

8.1.2. Identificación de requisitos de seguridad

A. Objetivo

Establecer requisitos de seguridad desde el inicio del desarrollo y durante el ciclo de vida del sistema.

B. Aplicabilidad

Desarrollo y mantenimiento de sistemas.

C. Directrices

i. Identificar requisitos de seguridad para el desarrollo y mantenimiento de sistemas. Una forma de identificar es consultando los registros de incidentes, el valor de la información que representa para entidad o institución pública, las vulnerabilidades conocidas y/o requisitos de las partes interesadas.
ii. Evaluar la criticidad de la información en términos de confidencialidad, integridad y disponibilidad para dotar de mayores controles de seguridad.
iii. Los requisitos de seguridad deberán contemplar requerimientos de infraestructura tecnológica como disponibilidad y redundancia de almacenamiento.
iv. Considerar como requisito la identificación de tipos de usuarios, autorización, autenticación, ambientes de desarrollo, pruebas y despliegue a producción.
v. Identificar requisitos criptográficos y firma digital.
vi. Las partes interesadas deberían formar parte integral durante el proceso de desarrollo.
vii. Las partes interesadas deberán coordinar temas relacionados a seguridad, funcionalidad, usabilidad y otros.
viii. Considerar la protección y privacidad de los datos personales recolectados a través de las aplicaciones.

8.1.3. Seguridad en el desarrollo y mantenimiento de sistemas

A. Objetivo

Asegurar el desarrollo y mantenimiento de sistemas para evitar un impacto operacional adverso.

B. Aplicabilidad

Desarrollo y mantenimiento de sistemas.

C. Directrices

i. Establecer procesos/procedimientos para técnicas de programación segura.
ii. Se deberán separar los ambientes de desarrollo, pruebas y producción.
iii. El proceso de desarrollo deberá contar con la documentación necesaria.
iv. Establecer procedimientos para el control de cambios, uso de repositorios seguros, documentar cambios funcionales y de seguridad a producción.
v. Los cambios a producción deberán ser autorizados y documentados previa realización de pruebas.
vi. El uso de librerías de terceros deberían ser evaluadas en relación a la funcionalidad, seguridad, fuentes confiables y referenciados localmente.
vii. Elaborar procesos/procedimientos de actualización de seguridad para librerías, bases de datos y software dependiente.

viii. Establecer procesos/procedimientos para la realización de copias de seguridad, estos deben contemplar el medio de almacenamiento, el ambiente y la frecuencia de las copias.
ix. De acuerdo a los requerimientos institucionales, se deberá considerar implementar medidas de seguridad para el acceso físico/lógico a los recursos de los ambientes de desarrollo, pruebas y producción según corresponda.
x. Se deben validar datos de entrada y salida, porque este tema es parte de las vulnerabilidades conocidas de los sistemas.
xi. Los procedimientos de desarrollo de sistemas deben aplicar técnicas de ingeniería segura que brinden orientación sobre las técnicas de autentificación, control, validación de datos, sanitización y eliminación de código de depuración.

8.1.4. Interoperabilidad de sistemas

A. Objetivo

Asegurar la transacción e intercambio de información entre sistemas de información.

B. Aplicabilidad

Sistemas que consumen o proveen información a otros sistemas.

C. Directrices

i. Utilizar técnicas de cifrado para transacción e intercambio de información que preserve la confidencialidad e integridad de la información.
ii. La información de autenticación de usuarios deberá ser válida y verificable.
iii. Utilizar protocolos de comunicación cifrada.
iv. Se deberán establecer términos y condiciones de uso del servicio entre las partes.
v. La protección de la información de los sistemas puede involucrar la transferencia o el acceso de la información desde puntos externos o fronteras. En este caso la institución debe tener conocimiento de las responsabilidades legales y contractuales para seguridad de la información

8.1.5. Pruebas de seguridad

A. Objetivo

Evaluar la seguridad de los sistemas.

B. Aplicabilidad

Desarrollo, mantenimiento y adquisición de sistemas.

C. Directrices

i. Las pruebas de seguridad se deberán especificar desde el diseño del sistema y realizarse durante el desarrollo del mismo.
ii. Para las pruebas se deberán tomar como referencias las vulnerabilidades conocidas.
iii. Documentar las pruebas de aceptación para desarrollos internos y externos, de acuerdo a los requisitos de seguridad establecidos.

iv. Las pruebas deberán permitir evaluar el cumplimiento de la normativa de desarrollo en cuanto a buenas prácticas de codificación e identificar código malicioso.
v. Las pruebas se deberán realizar utilizando herramientas como analizadores de código, escáneres de vulnerabilidades y otros.
vi. El ambiente de pruebas deberá estar configurado con las mismas características de seguridad al ambiente de producción.
vii. Las pruebas deben considerar canales ocultos para prevenir accesos no autorizados, monitoreo, validación, denegación de servicios, suplantación.

8.1.6. Seguridad en bases de datos

A. Objetivo

Gestionar y documentar la seguridad en bases de datos.

B. Aplicabilidad

Bases de datos

C. Directrices

i. Aplicar recomendaciones de configuración en seguridad provistas por el desarrollador del gestor de base de datos.
ii. Considerar implementar redundancia y alta disponibilidad según requisitos de seguridad establecidos.
iii. Para la gestión de copias de respaldo, se deberán elaborar procesos / procedimientos que establezcan responsables, periodicidad y otros que se considere necesario.
iv. Gestionar usuarios y privilegios para acceso a bases de datos, tablas, funciones y otros.
v. Las cuentas de usuario deberán tener propietarios con responsabilidades de uso.
vi. Para el acceso de cuentas de usuarios a las bases de datos en ambientes de desarrollo, pruebas y producción, se deberán implementar controles de autenticación y autorización.
vii. La extracción de datos de producción para las pruebas de funcionalidad deberán considerar la confidencialidad de la misma y los controles necesarios para resguardarla.
viii. Se deberán optimizar las consultas lógicas a bases de datos.
ix. Restringir el uso de cuentas de usuario por defecto.
x. En caso de cambios y/o modificaciones a las bases de datos se deberán realizar pruebas de aceptación y funcionalidad bajo autorización documentada.

8.2. Seguridad para la adquisición de sistemas

Establecer requisitos de seguridad para la adquisición de sistemas, software y aplicaciones a terceros.

8.2.1. Requisitos de seguridad

A. Objetivo

Contemplar requisitos de seguridad para la adquisición de sistemas, software y aplicaciones.

B. Aplicabilidad

Adquisición de software, sistemas y aplicaciones.

C. Directrices

i. Se deberán establecer los requerimientos de seguridad y aceptación de acuerdo a la normativa de desarrollo institucional en los términos de referencia.
ii. Comunicar la normativa de desarrollo a las partes interesadas en el proceso de adquisición y/o desarrollo terciarizado.
iii. Se deberán establecer acuerdos de nivel servicio (SLA) con la parte interesada.
iv. Debe obtenerse en la medida de lo posible, información oportuna de las vulnerabilidades técnicas de los sistemas, software y aplicaciones a ser adquiridos de terceros, así como la información relevante con respecto a actualizaciones y parches.

9. Gestión de incidentes de seguridad de la información

Establecer mecanismos para la gestión de incidentes en seguridad de la información dentro de la institución o entidad pública para dar continuidad a las operaciones y mejorar los controles de seguridad implementados.

9.1. Gestión de incidentes de seguridad de la información

Reducir la afectación negativa a la seguridad de la información y/o continuidad de las operaciones de la entidad o institución pública.

9.1.1. Plan de gestión de incidentes

A. Objetivo

Establecer lineamientos, roles, responsabilidades y procedimientos en la gestión de incidentes, para una respuesta eficaz ante la ocurrencia de eventos adversos relacionados a la seguridad de la información.

B. Aplicabilidad

Incidentes en seguridad de la información.

C. Directrices

i. Se deberá elaborar procesos y/o procedimientos de gestión de incidentes de seguridad de la información, los mismos deben establecer roles, responsabilidades informar, evaluar y responder sobre eventos de seguridad.
ii. El RSI deberá identificar el incidente para registrar el mismo, el tratamiento que se le dío y/o escalamiento.
iii. El RSI deberá evaluar cada evento de seguridad clasificarlo para su reporte.
iv. Los incidentes que no puedan ser solucionados deberán ser escalados al Centro de Gestión de Incidentes Informáticos por el RSI.
v. El documento de reporte de incidentes y vulnerabilidades deberá ser socializado a los servidores públicos para que los mismos conozcan los medios de reporte.
vi. Ante la ocurrencia de incidentes se deberá recuperar y restablecer la operatividad normal de activos de información.

vii. El RSI deberá ser el punto de contacto al interior de la institución y con Responsables de Seguridad de la Información de entidades públicas.
viii. Una vez que haya pasado el incidente, se deberán documentar las actividades de respuesta.
ix. Se deberá llevar una bitácora de eventos para el análisis posterior sobre los costos asociados al incidente y sobre los cuales se deben implementar soluciones a corto, mediano y largo plazo para reducir la probabilidad de ocurrencia futura.
x. El RSI deberá nominar al personal de respuesta ante incidentes, con la responsabilidad, la autoridad y la competencia necesaria para administrar un incidente y mantener la seguridad de la información.
xi. El RSI deberá establecer, documentar, implementar y mantener los procesos, procedimientos y controles para dar respuesta a incidentes de Seguridad de la Información.
xii. En caso de ser necesario la institución debe realizar, acorde al incidente, un proceso para administrar y gestionar la evidencia forense.
xiii. En un proceso de atención a incidentes, el RSI en caso de requerir evidencia forense, podrá involucrar a un abogado o la Policía Nacional para el comienzo de acciones legales o asesoría sobre la evidencia.

10. Plan de contingencias tecnológicas

Implementar un Plan de Contingencias Tecnológicas que permita controlar un incidente de seguridad de la información o una situación de emergencia, minimizando sus consecuencias negativas. Asimismo deberá determinar sus requisitos para la seguridad de la información ante situaciones adversas.

10.1. Implementación del plan de contingencias tecnológicas

La entidad o institución pública debe contar con un Plan de Contingencias Tecnológicas formalizado, actualizado e implementado; aprobado por el Comité de Seguridad de la Información, asignando responsabilidades para su ejecución a los propietarios de los activos de información.

10.1.1. Elaboración del plan de contingencias tecnológicas

A. Objetivo

Definir las estrategias, acciones, procedimientos y responsabilidades para minimizar el impacto de una interrupción imprevista de las funciones críticas y conseguir la restauración de las mismas, dentro de los límites de tiempo establecidos.

B. Aplicabilidad

El plan de contingencias está circunscrito a los eventos tecnológicos.

C. Directrices

i. Para la elaboración del Plan de Contingencias Tecnológicas se debe considerar: el análisis y evaluación de riesgos en

seguridad de la información; la mejora continua a partir de la Gestión de Incidentes de Seguridad de la Información; la determinación de los eventos que afecten la operación de los sistemas de información; la determinación de los procesos, operaciones críticos y los recursos tecnológicos asociados a estos.

ii. Implementar procesos y/o procedimientos de recuperación y restauración de operaciones críticas para cada evento identificado.
iii. Cada documento operativo debe incluir responsabilidades, procedimientos, funciones e identificación del personal que ejecutará el plan.
iv. Los responsables de activos de información en coordinación con el Comité de Seguridad de la Información definen los tiempos máximos de restauración.
v. La entidad o institución pública deberá identificar los requisitos institucionales para la disponibilidad de los sistemas de información.
vi. Cada Plan de Contingencias Tecnológicas deberá describir el enfoque para la continuidad, así como las condiciones necesarias para activar un plan de escalamiento si fuese necesario.

10.1.2. Pruebas y mantenimiento del plan de contingencias tecnológicas

A. Objetivo

El Plan de Contingencias Tecnológicas debe ser sujeto a revisiones periódicas y ejercicios de entrenamiento para asegurar su actualización.

B. Aplicabilidad

Aplica al Plan de Contingencias Tecnológicas y a los servidores públicos involucrados en el plan.

C. Directrices

i. El RSI coordinará de manera periódica la ejecución de las pruebas al Plan de Contingencias Tecnológicas para verificar, revisar y evaluar el mismo.
ii. Producto de las pruebas, el RSI podrá incorporar situaciones no cubiertas al plan.
iii. En caso de que las pruebas no sean exitosas, el RSI deberá gestionar la implementación de acciones correctivas o preventivas y ejecutar nuevamente las pruebas hasta cumplir con el objetivo planteado.
iv. Se debe documentar la realización de las pruebas y la implementación de los planes de acción correctivos o preventivos según correspondan.
v. El RSI, en coordinación con los involucrados, debe realizar revisiones periódicas al Plan de Contingencias Tecnológicas en función a la gestión de incidentes de seguridad de la información y al tratamiento de riesgos tecnológicos.

11. Cumplimiento

Asegurar el cumplimiento operativo del Plan Institucional de Seguridad de la Información que conlleva la Política de Seguridad y la documentación resultante de la misma.

11.1. Revisión de controles

Evaluar periódicamente el cumplimiento de la normativa documental del Plan Institucional de Seguridad de la Información, verificando que los mismos se encuentran en operación.

11.1.1. Revisión

A. Objetivo

Validar el cumplimiento de los controles de seguridad implementados.

B. Aplicabilidad

Plan Institucional de Seguridad de la Información.

C. Directrices

i. El Responsable de Seguridad de la Información, en coordinación con el Comité de Seguridad de la Información, será el encargado de verificar la correcta implementación, aplicación y cumplimiento, debiendo realizar revisiones y evaluaciones periódicas al Plan Institucional de Seguridad de la Información, en las que tomará en cuenta los siguientes criterios.

ii. Identificar causas del incumpliendo.

iii. Acciones para lograr el cumplimiento.

iv. Implementar acciones correctivas y preventivas para lograr un proceso continuo, iterativo y de mejora continua del PISI.

v. Revisar el cumplimiento de las acciones correctivas o preventivas.

vi. Los propietarios de procesos, activos de información e información serán los responsables del cumplimiento de las acciones correctivas.

vii. El RSI informará al CSI el estado de cumplimiento de los controles de seguridad implementados.

11.1.2. Verificación del cumplimiento técnico

A. Objetivo

Detectar vulnerabilidades técnicas en la infraestructura tecnológica.

B. Aplicabilidad

Tecnologías de la Información.

C. Directrices

i. Realizar evaluaciones de vulnerabilidades técnicas y hacking ético.

ii. Los resultados de la evaluación deben permitir identificar debilidades de seguridad para mitigar los mismos en el corto, mediano y largo plazo.
iii. Solicitar a la AGETIC u otras entidades la realización de evaluaciones de seguridad de la información, infraestructura, sistemas informáticos entre otros, en coordinación con el personal de la entidad pública que lo requiera.
iv. Realizar revisiones de cumplimiento técnico que también involucra una revisión de los sistemas operacionales críticos y sensibles para ver que estos se hayan implementado de forma correcta.

11.2. Auditoría al Plan Institucional de Seguridad de la Información

Verificar el cumplimiento del Plan Institucional de Seguridad de la Información.

11.2.1. Evaluación de cumplimiento del plan Institucional de seguridad de la información

A. Objetivo

Evaluar el grado de cumplimiento del Plan Institucional de Seguridad y las métricas determinadas para cada control implementado por la entidad.

B. Aplicabilidad

Plan Institucional de Seguridad de la Información

C. Directrices

i. La unidad de auditoría interna será la encargada de la revisión de cumplimiento del Plan de Seguridad Institucional de la Información relacionado con los documentos normativos, operativos y métricas.
ii. En caso de ser necesario la unidad de auditoría interna podrá delegar a un especialista la revisión para identificar debilidades técnicas y operativas en los controles para la mejora continua de los mismos.
iii. La entidad o institución pública podrá presentar a la AGETIC los avances en el desarrollo e implementación del Plan Institucional de Seguridad de la Información.
iv. La entidad o institución pública presentará a la AGETIC el Plan Institucional de Seguridad de la Información, de acuerdo a normativa legal vigente en el Estado Plurinacional de Bolivia.