2017

Instituto de Acceso
a la Información Pública

Plan de seguridad de la información digital

UNIDAD DE INFORMÁTICA

IAIP | Prolongación Avenida Masferrer y Calle al Volcán No. 88, Edificio Oca Chang, Col. San Antonio Abad.
| Correo: info@iaip.gob.sv | PBX: (503)2205-3800 | Fax: (503) 2205-3880 Buzón: 901

Aprobación de documento

Elaboró: Ing. Jorge Martínez Jefe de Unidad de Informática Febrero 2017	**Revisó:** Ing. José Juan Marroquín Director Ejecutivo Febrero 2017	Autorizó Lic. Hernán Gómez Comisionado Presidente en funciones Marzo 2017

Ediciones y/o revisiones

Edición	Revisión	Fecha emisión	Cambios realizados
01	01	Marzo 2017	Versión inicial

Contenido

Introducción

El presente documento se constituye en un instrumento necesario para contribuir a la seguridad de la información en el Instituto de Acceso a la Información Pública.

El IAIP como todas las instituciones y entidades de la administración pública se enfrentan a una variedad de amenazas que ponen en riesgo de forma directa o indirecta los datos personales y la información que se produce, transmite y resguarda, así como los recursos tecnológicos con los que se desarrollan las actividades antes mencionadas.

El plan de seguridad tiene como objetivo determinar y reducir el riesgo, mantener la integridad de la información que se genera, transmite y resguarda en el Instituto en formato electrónico. Con lo anterior reducir los daños o pérdida de la información y mantener la continuidad de las operaciones institucionales.

Ante esta situación el IAIP considera la información como un elemento activo y de vital importancia, por eso es necesario establecer criterios que garanticen la reducción de las amenazas a la información y permitan una gestión segura de los procesos, ofreciendo un mayor grado de seguridad a la información.

Para el desarrollo del plan de seguridad de la información se han considerado los lineamientos de tecnologías de la información y comunicación – LITIC – establecidos por el Instituto como documentación base y de soporte para este documento.

Objetivos

Objetivo General

Promover la importancia de la seguridad de la información y la gestión necesaria para reducir las amenazas que ponen en riesgo la información digital generada, transmitida y en resguardo del Instituto.

Objetivos Específicos

a) Evaluar e identificar posibles riesgos de seguridad de información.
b) Proteger los activos de información, con base a criterios de confidencialidad, integridad, reserva, protección de datos personales y disponibilidad.
c) Proteger los activos físicos de tecnología para reducir los riesgos de pérdida o daño en la información.

Alcance

Este documento está dirigido a todo el personal del IAIP, además deberá ser acatada por todas aquellas personas que en el ejercicio de sus labores hagan uso de las instalaciones, tengan acceso a la información, los servicios y recursos de Tecnología de Información y Comunicación de la Institución en forma directa (empleados, pasantes y practicantes) como indirecta (visitas, otros).

Marco legal

Normativa del Instituto de Acceso a la Información Pública

Normas Técnicas de Control Interno – NTCI –

Artículo 32. Proceso de identificación, registro y recuperación de la información.

Artículo 33. Características de la información.

Artículo 34. Efectiva comunicación de la información.

Corte de Cuentas de la República

Decreto N° 24. Reglamento para el uso y control de las tecnologías de la información y comunicación en las entidades del sector público.

Glosario

- IAIP: Instituto de Acceso a la Información Pública
- Plan de seguridad de la información: es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.
- Confidencialidad: es la propiedad que impide la divulgación de información a individuos, entidades o procesos no autorizados
- Integridad: Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas
- Disponibilidad: es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.
- Amenaza: hecho que puede producir un daño provocado por un evento natural o a causa de actividad humana.
- Riesgo: Es la materialización de vulnerabilidades identificadas, asociadas con su probabilidad de ocurrencia, amenazas expuestas, así como el impacto negativo que ocasione a las operaciones de negocio.
- Información digital: El concepto de información digital se aplica para todo aquello que está representado mediante ceros y unos dentro de una computadora. La información digital no sólo son textos electrónicos, también se incluyen las imágenes, el audio y el video, que al igual que los textos tienen diferentes formatos, codificaciones y representaciones en el mundo electrónico
- Contraseña de alto nivel: se considera aquella que incluye minúsculas, mayúsculas, números y caracteres especiales.
- Dirección IP: es un número que identifica, de manera lógica y jerárquica, a una Interfaz en red.
- Proveedor ISP: es la empresa que brinda conexión a Internet a sus clientes. Un ISP conecta a sus usuarios a Internet a través de diferentes tecnologías como DSL, cable módem, GSM, dial-up, entre otros.

Generales

El Plan de seguridad de la información tiene como finalidad conservar la integridad, confidencialidad, reserva, protección de datos personales y disponibilidad de la información.

Con base a lo anterior la Unidad de Informática, con el apoyo constante de los comisionados, gerencias y jefaturas brinda el seguimiento de este plan y así, ofrecer de forma oportuna y segura los servicios a la población.

Es importante fortalecer la seguridad en los recursos tecnológicos institucionales con el único fin de reducir el nivel de riesgo que afecta a la información, para lo anterior, el Instituto considera como documento base los Lineamientos de Tecnologías de Información y Comunicación - LITIC.

Seguridad de la información

Para el IAIP la seguridad de la información es una gestión continua que permite preservar la integridad, confidencialidad, reserva y protección de datos personales. Lo anterior se alcanza mediante criterios establecidos que guían en la conservación de la información y acompañen al usuario para ofrecer la seguridad que el activo de información merece.

El plan de seguridad de la información está orientado a los riesgos y la prevención o reducción de los mismos, con las tecnologías de información y comunicación.

Antes de iniciar con la identificación de amenazas o riesgos es importante contar con un inventario del equipo tecnológico actualizado, con ello determinar los recursos necesarios para brindar mantenimiento y seguridad en la creación, reproducción y resguardo de la información. A continuación detalle del inventario:

N°	Descripción	Cantidad
1	Equipo de escritorio (Computadora)	38
2	Equipo portátil (Computadora)	16
3	Equipo de conmutación y enrutamiento	3
4	Access Point	6
5	Impresor	9
6	Escáner	2

Prevención de daños en equipo informáticos

1. Como parte de la protección de la información es importante brindar la protección y los mantenimientos preventivos y correctivos necesarios a los equipos informáticos.
2. Todo el equipo debe contar con equipó de protección eléctrica UPS
3. El área de telecomunicaciones debe contar con el equipo de protección eléctrica necesario para resguardar el equipo alojado en el cuarto.
4. El área de telecomunicaciones debe mantener una temperatura ambiente mínima de 21°C para el adecuado cuido del equipo de telecomunicaciones.

5. Los equipos informáticos no se deben instalar o ubicar en el piso bajo los escritorios, en casos de inundación o filtración de agua, estos se pueden ver afectados y dañados por completo.

Identificación de amenazas y riesgos:

Es importante para el IAIP identificar las posibles amenazas que afectan la información, estas pueden ser lógicas o físicas y se pueden presentar de forma natural, accidental o provocada.

A continuación se presentan algunas amenazas identificadas a la fecha:

Desastres, naturales o de infraestructura: todos aquellos provocados de forma fortuita en el que los equipos y la información se ven afectados de forma directa o indirecta. Entre ellos podemos mencionar: inundaciones, incendios, cortocircuitos, sobre carga, terremotos, etc.

Daños en los equipos informáticos y de telecomunicación: es todo aquel daño que es provocado por los imprevistos técnicos, tiempo de vida útil del equipo, conexiones eléctricas, planta eléctrica, conexión de banda ancha, etc.

Errores en la lectura y escritura de datos: eliminación o modificación voluntaria o involuntaria de información, accesos no autorizados, resguardo de información no adecuada, etc.

Sabotajes y robo de equipo informático o información: pérdida o robo de equipo o información, ataques de red, virus o programas mal intencionados, etc.

Prevención de amenazas o riesgos

Por medio de controles de acceso

Estos controles permiten al IAIP mantener la seguridad de la información bajo niveles restringidos en los cuales, el acceso a las instalaciones y oficinas, los equipos tecnológicos y la información física juegan un papel importante.

Para lograr un control de acceso oportuno es importante determinar criterios que permitan restringir la información únicamente al personal autorizado con base al perfil de acceso asignado. Los controles de acceso se dividen de la siguiente forma:

a. Acceso a las instalaciones

El acceso a las instalaciones del IAIP es el primer punto de alto riesgo que permite vulnerar la seguridad de la información, por eso, es importante el cierre adecuado de las instalaciones al finalizar la jornada laboral y durante la jornada se debe mantener un control de las personas que ingresan y el registro de estas al ingresar a las instalaciones. En ese sentido todas las unidades deben tener el control de las personas que ingresan a su unidad.

Los visitantes de la institución, deberán ser acompañados por el personal correspondiente durante el tiempo de estancia. Todos los visitantes sin excepción deberán ser acompañados.

Se deberá asignar una identificación a los visitantes del Instituto con el fin de conocer que unidad visita o que gestión realiza en las instalaciones del IAIP. Con base a lo anterior las identificaciones pueden ser: visita, proveedor, capacitación, cooperación, audiencias, prensa.

La seguridad de la información no depende únicamente del adecuado uso y seguimiento de los usuarios, también depende de la seguridad de las instalaciones, por lo que se han implementado a la fecha elementos como: sistema contra incendios, identificación de zonas de riesgo y de zonas restringidas, acceso controlado para empleados, identificación de visitantes, sistema de seguridad y monitoreo con el fin de mantener segura la información y el activo que la produce, almacena y transmite.

El área de telecomunicaciones se considera área crítica de acceso, por lo que únicamente la Unida de Informática, la Gerencia Administrativa y la Dirección Ejecutiva tienen acceso a este. Cualquier otra persona deberá justificar y solicitar la autorización correspondiente para su acceso.

b. Acceso a la información:

La información es uno de los activos más valorados del IAIP por los servicios que se brindan a la población, por ello es importante mantener la integridad y seguridad de la información.

Los accesos restringidos se determinan con base a las funciones que desarrollan las unidades y será el jefe de unidad el responsable de especificar la información y su uso adecuado.

Antes de enviar un correo electrónico con cualquier tipo de información, es importante verificar los destinatarios y el contenido del mismo para evitar envíos a personas ajenas a la información.

En los casos que el envío de información se realizó al destinatario equivocado, se debe notificar inmediatamente que la información recibida debe ser eliminada o reenviada a su remitente.

Las cuentas de correo electrónico de la institución deben contener una cláusula de confidencialidad en el pie de página.

Todo el personal que tenga en su custodia información es responsable de proteger la integridad de la misma por medio del acceso y modificación que puedan provocar pérdida, alteración, destrucción o uso no adecuado. El personal no debe compartir información a personas no relacionadas con el trabajo sin autorización previa.

Es responsabilidad del usuario que haga uso de la información en el equipo informático o sistemas informáticos velar por la integridad, confidencialidad y disponibilidad de la información, especialmente en los casos que se considere reservada o confidencial.

El acceso a la información y los sistemas informáticos se asignara según las funciones y la relación en los procesos, procedimientos o trámites que interactúan con la misma. Cualquier acceso y uso no autorizado será responsabilidad del usuario asignado y será sancionado con base al acuerdo de confidencialidad (ver anexo 1).

Todo el personal, incluyendo las pasantías deberá firmar un acuerdo de confidencialidad y será responsabilidad de los jefes de cada Unidad velar por el cumplimiento de dicho acuerdo. Esto con el objeto de reducir el daño, pérdida o robo de información, con ello determinar obligaciones y responsabilidades de los usuarios.

Para evitar el uso no autorizado de los equipos informáticos y el acceso a la información que está bajo custodia, se recomienda: guardar y cerrar el editor de texto, cerrar sesión de los sistemas informáticos y los recursos compartidos, bloquear el equipo en cada momento que se retira del puesto de trabajo (se recomienda el uso de la combinación de teclas "Windows + L" para el bloqueo del equipo).

c. Acceso lógico (internet, redes sociales, redes y recursos compartidos)

El personal del Instituto, personal en pasantías y visitas, tendrán acceso a los servicios de red, internet, y recursos compartidos específicos con los privilegios según su actividad laboral, lo anterior con base a los lineamientos establecidos en el documentos Lineamientos de Tecnologías de la Información y Comunicación – LITIC –

Es responsabilidad de las jefaturas establecer los tipos de accesos para los recursos compartidos.

El acceso a los recursos institucionales en línea como intranet, sitios web, entre otros, tendrán un usuario único, el cual se debe asignar con base a la función.

Es responsabilidad del usuario mantener sus credenciales de acceso seguras y crear una contraseña de alto nivel.[1]

La información que se brinda por medio de las redes sociales debe tener previa autorización para evitar publicaciones que puedan dañar la imagen del Instituto y la integridad de los servicios que se ofrecen.

Cualquier publicación a realizar en el sitio web o redes sociales se debe realizar con base a los lineamientos establecidos por la Unidad de Comunicaciones para el acceso, uso y publicación en las redes sociales.

[1] Contraseña de alto nivel se considera aquella que incluye minúsculas, mayúsculas, números y caracteres especiales.

Gestión de amenazas o riesgos

Ante cualquier situación de amenaza o riesgo potencial se debe considerar algunos pasos importantes para reducir el impacto en la institución.

En la siguiente información se definen algunos criterios importantes según el caso:

Desastres, naturales o de infraestructura

1. Informar al personal correspondiente.
2. En los casos que el incidente se de en jornada laboral, activar la alarma institucional y evacuar al personal.
3. En casos de inundación desconectar los equipos electrónicos, bajar los interruptores del tablero principal.
4. En casos de incendio, hacer el adecuado uso de los extintores según el caso en instalaciones y equipos electrónicos.
5. En casos de sobre carga eléctrica, verificar que los equipos de protección estén activos y de ser una falla constante se debe bajar los interruptores del tablero principal y desconectar los equipos protección eléctrica UPS.

Daños en los equipos informáticos y de telecomunicación

1. Notificar al jefe inmediato sobre el daño del equipo
2. Solicitar el apoyo de la Unidad de Informática para la revisión del equipo y determinar las posibles causas del daño.
3. Se proveerá equipo temporal en lo se brinda el soporte técnico y o reparación del equipo dañado.
4. En los casos que el daño sea provocado por fallas eléctricas se debe solicitar el apoyo de la Gerencia Administrativa para la revisión del o los toma corrientes que afectan el equipo.
5. Cuando se presenten dificultades con la conectividad a Internet, se debe informar a la Unidad de Informática para la revisión de los equipos y en los casos que sea necesario solicitar el apoyo inmediato del proveedor ISP[2]

Errores en la lectura y escritura de datos:

1. Cualquier caso que se presente en este apartado se debe notificar al jefe inmediato y suspender cualquier actividad que altere la información afectada.
2. El jefe de la Unidad Organizativa debe notificar a la Unidad de Informática para realizar el análisis correspondiente y determinar las posibles causas.
3. En los casos que se determine un acceso a la información no autorizado la Unidad de Informática brindará el soporte necesario para el cambio de credenciales del usuario afectado.
4. Es importante no manipular la información luego de detectar una variante en ella, esto con el fin de facilitar el uso de herramientas que permitan la recuperación o restauración de la información.

[2] ISP Proveedor de servicios de Internet por sus siglas en inglés.

Sabotajes y robo de equipo informático o información

1. En el caso de pérdida o robo de equipo informático, se debe notificar inmediatamente al jefe inmediato y a la Unidad de Informática.
    a. La Unidad de informática debe informar al responsable de activo fijo para seguir el proceso de a seguir con el proveedor de seguro y la baja de activo fijo.
    b. En los casos de pérdida o robo de terminales móviles, el usuario debe notificar a la empresa que provee el servicio y luego a su jefe inmediato. La Unidad de Informática realizará los procesos necesarios para la baja de los servicios y la aplicación del seguro del servicio y terminal.
2. En el caso que el usuario no encuentre la información completa o integra, deberá notificar a su jefe inmediato y a la Unidad de Informática
    a. El usuario no debe realizar ninguna acción en el equipo o documento en el que se ha detectado la falta o pérdida total de la información.
    b. La unidad de informática realizara los procesos necesarios para determinar la restauración o recuperación de la información.
3. En el caso de la detección de un posible ataque a la red del IAIP, la Unidad de Informática realizara los procesos necesarios para determinar si el ataque es interno o externo.
    a. En el caso de un ataque externo, se procede a cerrar los puertos de red y el bloqueo indefinido del sitio o la dirección IP[3] que está intentando ingresar.
    b. En el caso de un ataque interno se determina la dirección IP, se restringe el acceso y se procede a verificar la asignación de dicha IP.
    c. La Unidad de Informática verifica las posibles causas del ataque interno, virus en equipo o memoria USB, sitio web fraudulento.
4. En los casos de instalación de programas sospechosos, los usuarios deben notificar a la Unidad de Informática sobre las dificultades en el equipo informático.
    a. La Unidad de Informática hará una revisión completa del equipo informático afectado en busca de las posibles causas.
    b. Al determinar la causa, virus o programa malicioso, se procede a su eliminación.
    c. Al finalizar la limpieza del equipo se procede a verificar que la información y funcionamiento del equipo estén correctos. De lo contrario, se realizara respaldo de la información y realizará una instalación de sistema operativo y programas en el equipo.
    d. Al finalizar, se restara la información en el equipo.

En cada uno de los eventos presentados, se debe realizar el registro de cada incidente y la documentación correspondiente para facilitar la solución y seguimiento en los futuros casos.

[3] Dirección IP es un número que identifica, de manera lógica y jerárquica, a una Interfaz en red.

Actualización del documento

Este documento se actualizará al menos una vez al año, o en periodos menores con base a los sucesos que se presenten y la solución del mismo.

Seguimiento

Cronograma de seguimiento **Instituto de Acceso a la Información Pública** Unidad de Informática			
Actividad	Fecha anual		Responsable
	Inicio	Fin	
Revisión y actualización del plan de seguridad	agosto	septiembre	Unidad de Informática / Gerencia Administrativa
Verificación de cumplimiento de prevención de amenazas o riesgos	septiembre	octubre	Unidad de Informática / Gerencia Administrativa
Seguimiento de amenazas y riesgos	enero	diciembre	Unidad de Informática / Gerencia Administrativa

En el proceso de seguimiento de amenaza o riesgo, para cada incidente que se detecte o reporte se debe llevar un registro con los datos siguientes:

Registro de incidentes de seguridad **Instituto de Acceso a la Información Pública** Unidad de Informática					
Fecha	**Unidad**	**Evento**	**Acción realizada**	**Seguimiento programado**	**Firma**

Reporte de incidente: Nombre y firma

Responsable de IT: Nombre y firma

ANEXOS

Anexo 1

ACTA DE CONFIDENCIALIDAD

NOMBRE, EDAD, PROFESIÓN U OFICIO, DOMICILIO, DEPARTAMENTO, PORTADOR/A de mi Documento Único de Identidad número _____, DECLARO: **I)** Que a partir del día __ de ___ del año dos mil __, me encuentro vinculado a la Unidad _____ del Instituto de Acceso a la Información Pública (IAIP), en virtud de lo cual se me ha conferido acceso —digital, verbal o documental, directo o indirecto— a todo tipo de información incluyendo, de modo ejemplificativo, propiedad intelectual inscrita o por inscribirse en el registro correspondiente, literatura y documentación, creada, originada, producida, administrada o custodiada por el IAIP. Esta información y documentación está relacionada con el desempeño de labores dentro del IAIP y, en principio, es de uso estrictamente interno por lo que podría estar sujeta a confidencialidad o reserva, total o parcial. **II)** Que en virtud de lo anterior, EXPRESA Y FORMALMENTE ME COMPROMETO a dar cumplimiento a las condiciones siguientes: a) Guardar estricta confidencialidad y reserva de toda la información y documentación con tal carácter a la que tenga acceso en virtud de las labores que se me asignen, cuya divulgación no haya sido autorizada ni requerida por autoridad pública competente para ello; b) No divulgar a terceras personas, por ningún medio, información confidencial o reservada creada, originada, producida, administrada o custodiada por el IAIP de la que tenga conocimiento o a la que tenga acceso —sea verbal o escrito—, incluso al propio personal del IAIP que no tenga relación directa con el caso o actividad de que se trate; c) Utilizar la información exclusivamente para el desarrollo de las actividades que se me han encomendado, por lo que no podrá ser reproducida, divulgada ni sustraída total o parcialmente, por ningún medio, de cualquier soporte en que se encuentre, incluyendo los equipos informáticos, a menos que se trate de información pública o de información confidencial cuya divulgación ha sido autorizada; d) Cumplir con las medidas necesarias para el resguardo de la información y

documentación que ha sido puesta bajo mi custodia y/o manejo; e) Realizar todas las acciones necesarias para evitar la destrucción, alteración, sustracción, modificación, pérdida o cualquier otra acción que vulnere la integridad, calidad, seguridad y reserva de la información y documentación que ha sido puesta bajo mi custodia y/o manejo; f) No usar medios extraíbles y/o servicios en nube personales (cd's, dvd's, usb, discos externos, dropbox, drive, wuala, box, one drive, etc.) para almacenar información confidencial o reservada, creada, originada, producida, administrada o custodiada por IAIP, así como a no utilizar equipos personales para el desarrollo de labores o actividades asignadas con relación al IAIP, a menos que sea estrictamente necesario; g) Informar a quien corresponda sobre cualquier destrucción, alteración, sustracción, modificación, pérdida o cualquier otra acción que vulnere, dañe o ponga en riesgo la información y documentación creada, originada, producida, administrada o custodiada por IAIP, realizada por mí o por terceras personas, de la que tenga conocimiento; h) No publicar, divulgar o realizar comentarios relacionados con información reservada o confidencial de la cual he tenido conocimiento, por cualquier medio electrónico o redes sociales, incluyendo mensajería instantánea (whatsapp, telegram, line, viber, hangouts, etc.), mientras conserve tal carácter; i) Mantener la vigencia de las obligaciones aquí contraídas aún después del cese de mi vinculación con el IAIP, cualquiera que ésta sea; j) En caso de incumplir con cualquiera de las condiciones antes señaladas, expresamente manifiesto comprender que podré ser sancionado/a administrativa, penal y/o civilmente, por parte de las autoridades competentes; k) En caso de promover alguna acción judicial de cualquier naturaleza en mi contra, señalo como domicilio especial el de la Ciudad de San Salvador a cuyos Tribunales me someto. Manifiesto comprender y aceptar la naturaleza vinculante del presente documento, así como la aplicabilidad de cada uno de los términos estipulados en él a partir de ésta fecha. San Salvador a los ___ días del mes de ___ del año dos mil ____.

DOY FE que la firma que calza en el anterior escrito es auténtica, por haber sido puesta en mi presencia, de su puño y letra por NOMBRE, EDAD, PROFESION U OFICIO, DOMICILIO, DEPARTAMENTO, a quien conozco e identifico por medio de su Documento Único de Identidad _____. San Salvador, a los _ días del mes de _ del año dos mil _.

Instituto de Acceso
a la Información Pública