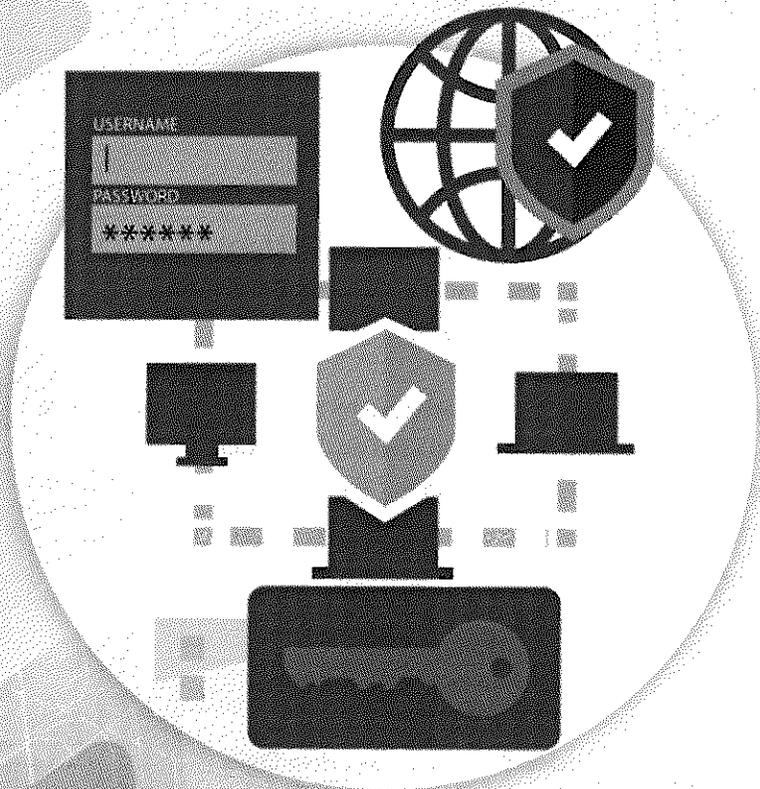




DIRECCIÓN GENERAL DE SERVICIO CIVIL



Documento Integral de Seguridad de la Información de la Dirección General de Servicio Civil de Costa Rica.

Disposiciones Generales para la Seguridad Física y Lógica de la Información

Ing. Reirier Hernández Li e Ing. Arnoldo Zambrano Madrigal
ÁREA DE DESARROLLO ESTRATÉGICO
Unidad de tecnologías de infocomunicación.

OCTUBRE 2016

FICHA DE CRÉDITOS

Documento elaborado por:

Ing. Reinier Hernández Li
Ing. Arnoldo Zambrano Madrigal

Documento revisado por:

Lic. Olman Luis Jiménez Corrales, MBA.

ÁREA DE DESARROLLO ESTRATÉGICO
Unidad de Tecnologías de Infocomunicación
- UTIC -

Documento Integral de Seguridad de la Información de la Dirección
General de Servicio Civil de Costa Rica.

Disposiciones Generales para la Seguridad Física y Lógica de la Información

Diseño Gráfico

Juan Pablo Barrientos Jiménez

Dirección General de Servicio Civil
San José, Costa Rica

- OCTUBRE 2016 -

TABLA DE CONTENIDO

Tabla de Contenido.....	1
Introducción.....	3
Objetivos	3
I. Sobre los recursos de la DGSC.....	3
A. Clasificación de los recursos de TI según su sensibilidad	3
B. Riesgos de los recursos de la DGSC.....	6
C. La Seguridad Informática Institucional.....	6
II. Sobre la Seguridad Física.....	6
A. Acceso al espacio físico de UTIC.....	6
B. Acceso al Cuarto de Servidores y Telecomunicación.....	6
C. Acceso a las computadoras personales.....	7
D. Manipulación de equipos de comunicación de la DGSC.....	8
E. Resguardo de los medios físicos de respaldo.....	8
F. Sobre los servidores.....	8
III. Sobre la Seguridad Lógica	9
A. Permisos, Roles y Usuarios	9
B. Sobre la Seguridad de la Información.....	11
C. Acceso a los equipos personales.....	11
D. Acceso a servidores	12
E. Acceso a servicios	12
F. Acceso a Internet	13
G. Acceso a administración de equipos de comunicación y seguridad	13
H. Sobre el uso del servicio de correo institucional	14
VI. Sobre el acceso al código fuente de las aplicaciones de la DGSC	14
Política.....	15
Obligaciones	15
V. Sanciones.....	15
VI. Continuidad de los servicios.....	15
A. Generalidades.....	15
B. Respaldo de datos	16
C. Manuales de instalación de los servicios institucionales	16
D. Capacitación.....	17

INTRODUCCIÓN

El siguiente documento nace a partir de los hallazgos encontrados por la auditoría llevada a cabo a los servicios que brinda la Unidad de Tecnologías de Infocomunicación (UTIC) mismos que deben ser atendidos con prontitud por tratarse de eventos que pueden desencadenar serios trastornos en el quehacer institucional en materia informática.

Pretendemos plantear soluciones a corto, mediano y largo plazo sobre aquellas falencias evidenciadas en el diagnóstico realizado a los servicios prestados por UTIC ya sea en software, hardware e infraestructura procurando resguardar el activo fundamental con que cuenta la Dirección General de Servicio Civil como son los datos que administra de los usuarios con los que interactúa cotidianamente.

Los puntos abordados en este instrumento han de servir como guía para los funcionarios de la UTIC así como para los usuarios institucionales sobre las políticas y herramientas necesarias que garanticen un mejor control sobre la información alojada en nuestros servidores institucionales.

OBJETIVOS

1. Generar políticas y procedimientos en materia de seguridad de la información para sistemas, infraestructura y sitio web institucionales.

2. Estimular el compromiso del personal de la DGSC con la seguridad de la información y confidencialidad y riesgos asociados con la información administrada por la institución.

3. Definir lineamientos claros sobre el control de acceso a la información (protección de la información) por parte de los usuarios internos y externos.

4. Generar alternativas para la continuidad en los servicios de TI y planes que documenten las acciones correctivas y preventivas.

5. Evaluar el impacto de los riesgos y clasificación de los recursos TI según criticidad.

I. SOBRE LOS RECURSOS DE LA DGSC

A. Clasificación de los recursos de TI según su sensibilidad

Actualmente la Unidad de Tecnologías de Infocomunicación debido a su naturaleza y funciones que desempeña se encuentra clasificada o subdividida de la siguiente manera:

- Administrador de servidores
- Administrador de comunicaciones
- Soporte técnico
- Analistas desarrolladores
- Web Master
- Administrador de Base de Datos

1. Servidor de Dominio	Brindar servicio de dominio, identificación y seguridad a los equipos dentro de su área.
Sensibilidad: Alta	Vulnerabilidad: Alta

Observaciones: Se requiere seguridad física garantizada que imposibilite el acceso al Hardware por parte de personal no autorizado. Requiere barreras de acceso lógico que impida el ingreso al sistema por parte de personal no autorizado. Este recurso es vulnerable a actualizaciones mal aplicadas, a virus informáticos y posible error humano en su administración. El fallo de este servidor tendría un altísimo impacto sobre la entrega de servicios institucionales y la capacidad de respuesta ante el usuario externo.

Custodia: UTIC	Responsabilidad: Administrador de Servidores
-----------------------	---

2. Servidor de Correo	Brindar servicio de correo a al recurso humano y los sistemas que lo requieran en la DGSC.
Sensibilidad: Media	Vulnerabilidad: Alta

Observaciones: Se requiere seguridad física garantizada que imposibilite el acceso al Hardware por parte de personal no autorizado. Requiere barreras de acceso lógico que impida el ingreso al sistema por parte de personal no autorizado. Este recurso es vulnerable a actualizaciones mal aplicadas, a virus informáticos y posible error humano en su administración. El fallo de este servidor impediría tanto a usuarios como a sistemas el enviar o recibir comunicaciones vía SMTP o POP3.

Custodia: UTIC	Responsabilidad: Administrador de Servidores
-----------------------	---

3. Servidor Antivirus	Brindar servicio de administración de los clientes antivirus instalados en los equipos de la DGSC.
Sensibilidad: Alta	Vulnerabilidad: Alta

Observaciones: Se requiere seguridad física garantizada que imposibilite el acceso al Hardware por parte de personal no autorizado. Requiere barreras de acceso lógico que impida el ingreso al sistema por parte de personal no autorizado. Este recurso es vulnerable a actualizaciones mal aplicadas, a virus informáticos y posible error humano en su administración. De fallar este servidor reduciría notablemente la confiabilidad y la efectividad del antivirus institucional, provocando severas grietas en la seguridad de los equipos personales.

Custodia: UTIC	Responsabilidad: Administrador de Servidores
-----------------------	---

4. Servidor de Archivos	Permitir el trabajo de múltiples recursos sobre un repositorio de documentos de nivel institucional.
Sensibilidad: Media	Vulnerabilidad: Alta

Observaciones: Se requiere seguridad física garantizada que imposibilite el acceso al Hardware por parte de personal no autorizado. Requiere barreras de acceso lógico que impida el ingreso al sistema por parte de personal no autorizado. Este recurso es vulnerable a actualizaciones mal aplicadas, a virus informáticos y posible error humano en su administración. Cualquier falla de este servidor podría dejar al recurso humano de la DGSC sin acceso a documentos sensibles para el desarrollo de las labores. Existe la probabilidad de pérdida de información por mal función de hardware o por un error humano.

Custodia: UTIC	Responsabilidad: Administrador de Servidores
-----------------------	---

5. Servidor de Virtualización	Generación y ejecución de ambientes virtuales para brindar diferentes servicios
Sensibilidad: Alta	Vulnerabilidad: Alta

Observaciones: Se requiere seguridad física garantizada que imposibilite el acceso al Hardware por parte de personal no autorizado. Requiere barreras de acceso lógico que impida el ingreso al sistema por parte de personal no autorizado. Este recurso es vulnerable a actualizaciones mal aplicadas, a virus informáticos y posible error humano en su administración. De fallar este servidor el impacto es variable, en dependencia de que servicios se estén virtualizando y la información contenida en ello.

Custodia: UTIC	Responsabilidad: Administrador de Servidores
-----------------------	---

6. Servidor de Base de Datos	Conservar y asegurar las características de la información y los datos.
Sensibilidad: Alta	Vulnerabilidad: Alta

Observaciones: Se requiere seguridad física garantizada que imposibilite el acceso al Hardware por parte de personal no autorizado. Requiere barreras de acceso lógico que impida el ingreso al sistema por parte de personal no autorizado. Este recurso es vulnerable a actualizaciones mal aplicadas, a virus informáticos y posible error humano en su administración. La función de este servidor lo convierte en uno de los blancos de seguridad más críticos. De fallar el servidor no solo se perdería la capacidad de entregar servicios sino que existe alto riesgo de perder datos. En dependencia del Sistema Gestor de Base de Datos que esté ofreciendo el servicio, su recuperación puede ser muy compleja.

Custodia: UTIC	Responsabilidad: Administrador de Base de Datos
-----------------------	--

7. Servidor de Aplicación	Publicar aplicaciones para que sean utilizadas por los usuarios designados.
Sensibilidad: Media	Vulnerabilidad: Alta

Observaciones: Se requiere seguridad física garantizada que imposibilite el acceso al Hardware por parte de personal no autorizado. Requiere barreras de acceso lógico que impida el ingreso al sistema por parte de personal no autorizado. Este recurso es vulnerable a actualizaciones mal aplicadas, a virus informáticos y posible error humano en su administración. Básicamente, la falla de este servidor afectaría la prestación de los servicios alojados en él. La magnitud de las repercusiones de un fallo de este servidor ira en dependencia de la importancia que tengan los servicios alojados en este. Al estar alojados en la DMZ, estos servidores son especialmente vulnerables a ataques. La recuperación de los servicios suele ser sencilla en comparación con otros servicios.

Custodia: UTIC	Responsabilidad: Administrador de Servidores y Analistas
-----------------------	---

8. Servidor de Respaldo	Brindar un respaldo de gran capacidad mediante un medio automático.
Sensibilidad: Media	Vulnerabilidad: Alta

Observaciones: Se requiere seguridad física garantizada que imposibilite el acceso al Hardware por parte de personal no autorizado. Requiere barreras de acceso lógico que impida el ingreso al sistema por parte de personal no autorizado. Este recurso es vulnerable a actualizaciones mal aplicadas, a virus informáticos y posible error humano en su administración. De fallar este servidor, la capacidad para recuperar información por causa de desastre se vería afectada y posiblemente suprimida.

Custodia: UTIC	Responsabilidad: Administrador de Servidores
-----------------------	---

9. Coordinador de TI	Organizar los esfuerzos y trabajos de los distintos recursos de TI para el logro de objetivos.
Sensibilidad: Alta	Vulnerabilidad: Alta

Observaciones: Como cualquier recurso humano, es sensible a la ingeniería social, al error y a la corrupción. La naturaleza de su rango, su capacidad para solicitar información técnica sin restricción y conocimiento a grandes rasgos de la arquitectura y manejo de datos lo convierten en un objetivo obvio de seguridad.

Custodia: N/A	Responsabilidad: Director de Área
----------------------	--

10. Administrador de Base de Datos	Administrar los sistemas gestores de base de datos y asegurar el correcto almacenamiento y seguridad de la información en las bases de datos
Sensibilidad: Alta	Vulnerabilidad: Alta

Observaciones: Como cualquier recurso humano, es sensible a la ingeniería social, al error y a la corrupción. El Administrador de Base de Datos es un punto crítico de seguridad de la información, al igual que lo es el Servidor de Base de Datos. Posee acceso y privilegios que le podrían permitir manipular libremente los datos requeridos por los servicios.

Custodia: N/A	Responsabilidad: Coordinador UTIC
----------------------	--

11. Webmaster	Codificar y diseñar soluciones y experiencias aplicadas a los sitios Web.
Sensibilidad: Baja	Vulnerabilidad: Alta

Observaciones: Como cualquier recurso humano, es sensible a la ingeniería social, al error y a la corrupción. Por su campo de acción, primariamente en los servidores de aplicaciones, sus capacidades para afectar las cualidades de la información deberían ser bajas y controladas, dejando únicamente posibilidades de afectar determinados servicios o comprometer información entrante al sistema.

Custodia: N/A	Responsabilidad: Coordinador UTIC
----------------------	--

12. Programador - Analista	Codificar y desarrollar soluciones según requerimientos de usuarios.
Sensibilidad: Baja	Vulnerabilidad: Alta

Observaciones: Como cualquier recurso humano, es sensible a la ingeniería social, al error y a la corrupción. Por su campo de acción, primariamente en los servidores de aplicaciones, sus capacidades para afectar las cualidades de la información deberían ser bajas y controladas, dejando únicamente posibilidades de afectar determinados servicios o comprometer información entrante al sistema.

Custodia: N/A	Responsabilidad: Coordinador UTIC
----------------------	--

13. Soporte técnico	Solucionar problemas percibidos por el recurso humano de la DGSC en sus equipos de trabajo, además de brindar mantenimiento a dicha equipación.
Sensibilidad: Baja	Vulnerabilidad: Alta

Observaciones: Como cualquier recurso humano, es sensible a la ingeniería social, al error y a la corrupción. No requiere contacto directo con la información. Por sus funciones no requiere acceso a roles elevados en los servicios o sistemas. Su contacto con el equipo de trabajo del recurso de la DGSC le abre la posibilidad de comprometer información localizada o proveniente de dicho equipo.

Custodia: N/A	Responsabilidad: Coordinador UTIC
----------------------	--

14. Encargado de Telecomunicaciones	Vigilar el funcionamiento de las redes de comunicaciones de la DGSC.
Sensibilidad: Alta	Vulnerabilidad: Alta

Observaciones: Como cualquier recurso humano, es sensible a la ingeniería social, al error y a la corrupción. Su acceso a la configuración de los equipos de comunicación y seguridad lo convierten en un blanco crítico de seguridad. Muchos de los ataques o delitos requieren los permisos que poseen los de este rol.

Custodia: N/A	Responsabilidad: Coordinador UTIC
----------------------	--

15. Administrador de Servidores	Vigilar la función de los servidores y los servicios que estos brindan
Sensibilidad:	Vulnerabilidad:

Observaciones: Como cualquier recurso humano, es sensible a la ingeniería social, al error y a la corrupción. Tiene acceso absoluto a las funciones dentro del Sistema Operativo y a los accesos de los servidores. Su conocimiento es crítico en la protección de la información y la prestación de servicios.

Custodia: N/A	Responsabilidad: Coordinador UTIC
----------------------	--

B. Riesgos de los recursos de la DGSC

Con la finalidad de mitigar el impacto que pueda tener la materialización de los riesgos no solo sobre los recursos de hardware, software e infraestructura, sino también sobre el recurso humano con que cuenta la DGSC; se hace necesaria la generación de medidas que contribuyan en su administración disminuyendo el impacto negativo que pueda ocasionar. Para ello establecemos los siguientes aspectos que año a año la UTIC debe velar por su cumplimiento y acatamiento obligatorio.

1. Elaborar anualmente un plan de riesgos por parte del Coordinador de TI el cual se clasifique en aquellos riesgos de hardware, software, infraestructura y recurso humano que pueda vislumbrarse y deba ser atendido.
2. Dar un seguimiento mensual a dicho plan de riesgos definiendo su atención para mitigar o resolver aquellos riesgos que se materialicen o puedan incorporarse como nuevos riesgos.
3. Ejecutar acciones que garanticen la eliminación o disminución del impacto del riesgo asociado.
4. Informar a las altas autoridades sobre las acciones y planes a seguir para atender los riesgos localizados buscando el apoyo necesario para su mitigación por medio de convenios con otras instituciones o apoyo de más personal.

C. La Seguridad Informática Institucional

Con el fin de garantizar la seguridad de la información para la Dirección General de Servicio Civil (DGSC), toda persona que ingresa y que utilice equipo y/o servicios informáticos debe aceptar las condiciones de confidencialidad, de uso de bienes y servicios informáticos, así como cumplir y respetar plenamente lo dispuesto en este documento.

II. SOBRE LA SEGURIDAD FÍSICA

A. Acceso al espacio físico de UTIC

La UTIC debe velar por la información y equipos que actualmente posee en su espacio físico razón por la que su acceso es restringido a personal no autorizado. Para llevar a cabo esta labor es necesario definir mecanismos físicos para acceder al sitio de trabajo de los miembros de UTIC así como al cuarto de servidores.

A continuación hemos definido una serie de puntos para implementar:

1. La solicitud de colaboración o resolución para la atención de problemas debe ser planteada a través de correo electrónico dirigiendo su atención al funcionario responsable.
2. Queda prohibido el acceso al lugar de trabajo de los funcionarios de UTIC por parte de los usuarios internos o externos, salvo que exista autorización expresa de la jefatura inmediata o superior de la UTIC.
3. Toda persona que deba reunirse con algún funcionario de UTIC debe plantear su solicitud por ventanilla y queda a discreción del profesional su respectiva atención.
4. Debe plantearse algún mecanismo de seguridad (llavín con apertura automático por ejemplo) para el ingreso de personal a las instalaciones físicas del personal de UTIC.

B. Acceso al Cuarto de Servidores y Telecomunicación

Se deben definir directrices que garanticen el resguardo del equipo ubicado en el cuarto de servidores de UTIC. Por ello hemos definido una serie de puntos para implementar, seguidamente se exponen:

5. El Cuarto de Servidores y Telecomunicación debe ser un área que disponga de medidas de seguridad, detección y extinción de incendios, clima controlado y adecuado según los requerimientos de los equipos informáticos, instalación eléctrica adecuada para el mantenimiento óptimo de los equipos y su función ininterrumpida y medidas de control de acceso de personal.
6. UTIC tiene la potestad, de acuerdo a sus funciones, para definir zonas restringidas que aseguren el control sobre el acceso de personal a bienes informáticos críticos. La definición de zonas restringidas tiene la finalidad de evitar accesos no autorizados a equipo crítico que puedan poner en riesgo la operación de la infraestructura informática o la pérdida de información.
7. Al crear una zona restringida, UTIC debe designar las excepciones de acceso correspondiente, según se amerite y se considere.
8. El acceso de personal no regular o externo a las zonas restringidas debe ser autorizado por el Coordinador de UTIC o Superior Inmediato según corresponda, previo justificación oficial. Está totalmente prohibido el acceso al Cuarto de Servidores y Telecomunicación a cualquier persona que no tenga autorización clara por parte del Coordinador de UTIC o por lo dispuesto en este documento.
9. Queda totalmente prohibido el ingreso con cualquier tipo de alimento o bebidas al Cuarto de Servidores y Telecomunicación.
10. Queda totalmente prohibido el fumar dentro del Cuarto de Servidores y Telecomunicaciones.
11. Cualquier persona externa a la institución que deba ingresar al Cuarto de Servidores, ya sea por una orden superior o por la prestación de servicios a la DGSC, debe presentar su identificación y quedar anotado en la bitácora de accesos. Debe presentar además documento que explique las razones por las que requiere ingresar, este documento será entregado al Coordinado de UTIC, quien debe avalar o no el ingreso. Además será acompañado en todo momento por el Administrador de Servidores.
12. Todo ingreso al Cuarto de Servidores y Telecomunicaciones debe quedar registrado con precisión en la Bitácora de Accesos al Cuarto de Servidores y Telecomunicación. Este registro será llevado por el Administrador de Servidores y en casos especiales por el Coordinador de UTIC.
13. Al registrar la salida de personal fuera de UTIC en la Bitácora de Accesos al Cuarto de Servidores y Telecomunicación, debe existir una firma de aprobación por parte del personal custodio indicado en el punto 7, asegurando la situación normal.
14. El personal regular autorizado para el ingreso al Cuarto de Servidores y Telecomunicación es:
 - a. El Coordinador de UTIC y Superior Inmediato.
 - b. Administrador de Servidores.
 - c. Encargado de Telecomunicaciones.
15. Cualquier persona, no mencionada en el punto anterior de acceso al Cuarto de Servidores y Telecomunicación, requiere autorización por parte del Coordinador de UTIC para acceder.

C. Acceso a las computadoras personales

Los bienes informáticos y sus componentes (hardware) asignados por la Dirección General de Servicio Civil a su personal para el desarrollo de sus deberes, es de custodia de cada depositario. Cualquier pérdida o daño a este equipo o alguna de sus partes será presumiblemente imputado al depositario salvo prueba de lo contrario. Los componentes (hardware) de los bienes informáticos debe ser inventariado antes de la entrega por Soporte Técnico. Este inventario servirá para posterior control al entregar y recibir el equipo de y hacia el colaborador asignado. El usuario debe notificar

oficialmente de inmediato la desaparición, pérdida, robo, extravío o daño de cualquier equipo informático o alguna de sus partes.

La entrega física de los bienes informáticos será realizada por personal del Área Administración de Servicios Institucionales.

La reubicación de equipo de informática debe ser autorizada por el Coordinador de UTIC o su Superior Inmediato cuando proceda, con previa valoración del Encargado de Telecomunicaciones, quien estudiará la viabilidad de la nueva localización según disponibilidad de puntos de acceso y la saturación de la red.

D. Manipulación de equipos de comunicación de la DGSC

Los equipos de comunicación estarán prioritariamente resguardados dentro del cuarto de comunicaciones, con excepción de aquellos que por su función o naturaleza requieran estar localizados en puntos comunes de la infraestructura de la DGSC, en cuyo caso deben estar debidamente resguardados y fuera del alcance del personal que no pertenece a UTIC.

Queda totalmente prohibido a personal no autorizado por el Coordinador de UTIC o este documento el manipular los equipos de comunicación.

E. Resguardo de los medios físicos de respaldo

La institución de velar por resguardo externo (fuera de sus instalaciones físicas) de las cintas de respaldo realizadas por la UTIC. Por tal motivo se establece el siguiente procedimiento para su puesta en práctica:

1. La UTIC debe elaborar un plan de respaldos y restauración anual el cual atenderá y ejecutará emitiendo informes semestrales sobre su aplicación y resultados obtenidos.
2. La UTIC realizará respaldos diarios de la información almacenada en sus servidores de base de datos.
3. Semanalmente se ha de realizar un respaldo total de dicha información el cual debe coordinarse con una empresa externa su respectivo almacenamiento.
4. La UTIC solicitará una copia de respaldo de dicha información a la empresa externa con la intención de realizar una restauración de la información almacenada previamente corroborando que las cintas están en perfectas condiciones y que la información esta correcta.
5. La UTIC debe montar un laboratorio de pruebas en el cual simular la restauración de la cinta y los usuarios verificar la veracidad de la información.

F. Sobre los servidores

Con la finalidad de asegurar un mejor desempeño de los servidores institucionales ubicados físicamente en la UTIC, se establecen los siguientes puntos a considerar:

1. Los servidores cuya función o uso sea crítico deberán obligatoriamente estar alojados en el cuarto de servidores, con el fin de brindar seguridad física, mejores condiciones ambientales, mejor condición de alimentación eléctrica y acceso solo de personal autorizado.
2. Cualquier cambio, reubicación, salida o baja de equipo de informática debe estar autorizado por el Coordinador de UTIC y sustentado mediante oficio, indicando en el mismo la marca, modelo, número de inventario, serie y características que ayuden a su completa descripción. Este oficio será copiado también a Proveeduría.
3. Se debe asegurar la regularidad y calidad del fluido eléctrico destinado a dar función al equipo informático.
4. Los servidores deben conservarse lejos de objetos magnéticos que puedan alterar su función o la confiabilidad de la información.
5. Soporte Técnico debe contar con un Plan de Mantenimiento Preventivo de Bienes Informáticos que contemple la limpieza y revisión periódica de los servidores y equipos dentro del Cuarto de Servidores y Comunicación.

6. Cuando se deba realizar mantenimiento preventivo sobre algún servidor o equipo de comunicación, se deberá notificar al Coordinador de UTIC quien a su vez comunicará oficialmente por el medio que considere conveniente a los usuarios o áreas que pudiesen resultar afectadas por la interrupción de los servicios prestados por los equipos que estarán en mantenimiento. Se debe indicar la hora de interrupción y el tiempo aproximado en el que el servicio no estará disponible.
 7. En el mantenimiento de cualquier servidor o equipo de comunicación bajo custodia de UTIC deben estar presentes el Administrador de Servidores y el Encargado de Telecomunicaciones, no importando si dicho mantenimiento es ejecutado por Soporte Técnico o un servicio externo. El Administrador de Servidores y el Encargado de Telecomunicación tienen como deber el asegurar que los equipos y servicios vuelvan al 100% de su funcionalidad después del mantenimiento.
 8. Queda totalmente prohibido a cualquier persona que no esté autorizada por el Coordinador de UTIC o lo descrito en este documento a manipular de cualquier forma los servidores institucionales.
3. Las solicitudes para nuevos usuarios de dominio cuyo fin sea garantizar a un colaborador de la DGSC el acceso a los servicios del dominio, deben ser remitidas por Recursos Humanos mediante solicitud formal según lo dispuesto en el punto 2.
 4. Solo podrán contar con rol de "Administrador de Dominio" los siguientes recursos:
 - a. Coordinador de UTIC
 - b. Administrador de Servidores
 - c. Encargado de Telecomunicaciones
 - d. Encargado de Seguridad
 5. Todos los usuarios de dominio que no estén listados en el punto anterior, salvo excepciones justificadas y aprobadas por el Coordinador de UTIC, deben pertenecer al grupo "Usuarios de Dominio" que tiene potestades reducidas.
 6. Las contraseñas usadas en usuarios de dominio deben cumplir con las siguientes características mínimas:
 - a. Tener al menos 8 caracteres.
 - b. Contar con al menos un número.
 - c. Contar con al menos una letra.
 - d. Contar con al menos una letra mayúscula.
 - e. Contar con un carácter especial que son el asterisco (*), el slash (/) o la arroba (@).
 - f. No debe contener espacios u otros signos no especificados en los puntos anteriores.
 7. Los usuarios de dominio generados primariamente contarán con una contraseña genérica que será asignada por el Administrador de Servidores. El usuario final del usuario de dominio tiene la obligación y total responsabilidad de cambiar la contraseña y colocar una nueva que cumpla con lo estipulado en el punto anterior.

III. SOBRE LA SEGURIDAD LÓGICA

A. Permisos, Roles y Usuarios

Respecto a los permisos, roles asignados a los usuarios, se establece la siguiente información:

1. Los usuarios de dominio serán creados exclusivamente por el Administrador de Servidores.
2. Para crear un usuario de dominio nuevo, se debe dirigir al Administrador de Servidores una solicitud formal, con copia al Coordinador de UTIC quien tendrá potestad para denegar la solicitud, indicando el usuario, área o sistema al que pertenece, responsable del usuario de

8. Es obligación absoluta del usuario de la cuenta de dominio el proteger la contraseña y asegurarse de ser el único quien conozca dicha información. Cuando el usuario dude acerca de la seguridad de la contraseña deberá notificar de inmediato al Administrador de Servidores para realizar el cambio.
9. Es obligación absoluta del usuario de la cuenta de dominio su uso, aprovechamiento y resguardo. Cuando exista sospecha sobre el uso de su cuenta de dominio por parte de otra u otras personas deberá notificarlo de inmediato al Administrador de Servidores para la destrucción de la cuenta y la generación de una nueva.
10. El Administrador de Servidores debe asegurar que las contraseñas de acceso a los usuarios de dominio con roles de administración y aquellos usuarios utilizados para la administración de equipos y servicios cumplan con los estándares de seguridad.
11. El usuario de dominio "Administrador" o "Administrator" debe estar deshabilitado y con una contraseña de alta seguridad, la cual solo debe ser de conocimiento de el Administrador de Servidores, el Encargado de Seguridad y el Coordinador de UTIC. Dicha contraseña debe estar anotada en un documento resguardado.
12. Los Administradores de Dominio deben siempre, sin excepción, utilizar su usuario de dominio para realizar sus labores y nunca se debe usar el usuario "Administrator" o "Administrador". Este punto busca llevar control de acceso y responsabilidad sobre los cambios y administración en el dominio.
13. El Administrador de Servidores será el único habilitado para cambiar contraseñas de los usuarios de dominio, pero solo en los casos con explícito consentimiento del colaborador responsable a quien fue asignado el usuario o por una orden superior oficializada y debidamente documentada aprobada por el Coordinador de UTIC.
14. El Administrador de Servidores no puede cambiar la contraseña arbitrariamente de un usuario de dominio utilizado por un sistema o en el desarrollo de sistemas sin consultar debidamente al responsable del sistema en UTIC e informar al Coordinador de UTIC.
15. Cualquier usuario local de un servidor que sea necesitado para la prestación de servicios debe tener no más que los roles mínimos requeridos para el cumplimiento de su función.
16. El usuario "Administrator" o "Administrador" local de los servidores debe ser deshabilitado y su contraseña debe ser cambiada por una de alta seguridad, la cual solo debe ser de conocimiento del Administrador de Servidores, el Encargado de Seguridad y el Coordinador de UTIC. Dichas contraseñas deben estar anotadas en un documento resguardado.
17. Las contraseñas utilizadas en los sistemas, bases de datos y servicios debe cumplir con lo anotado en el punto 7.
18. Las cuentas de dominio utilizadas por personal fuera de UTIC deberán cambiar contraseña en un plazo no mayor a 60 días. Para ello se habilitará la opción para que los usuarios procedan automáticamente a atender la solicitud del sistema.
19. Recursos Humanos está en la obligación de solicitar la creación de un nuevo usuario de dominio, así como de solicitar su cancelación cuando ya no sea necesaria. Igualmente cualquier miembro de UTIC que haya solicitado un usuario está en obligación de informar al Administrador de Servidores cuando dicho usuario ya no sea útil.
20. Es obligación de los funcionarios de la Dirección General de Servicio Civil el identificarse para el uso de los Servicios Informáticos mediante los medios y procedimientos que UTIC considere convenientes para asegurar la validez de la identidad.

B. Sobre la Seguridad de la Información

Todos los funcionarios de la Dirección General de Servicio Civil están en la obligación irrenunciable de proteger la información utilizada, transmitida y/o contenida en la infraestructura tecnológica de la DGSC. Así mismo, se debe proteger la información de los clientes y aquella que sea considerada crucial, reservada o confidencial que por responsabilidad institucional deba ser resguardada.

Cuando un funcionario conozca sobre un caso donde información sensible de la DGSC o de sus usuarios haya sido comprometida, revelada, modificada, alterada o eliminada sin autorización expresa, oficial y documentada de los jerarcas correspondientes, el usuario debe notificar al Director de Área correspondiente y a UTIC. Además, los Directores de área y jefaturas tienen la obligación de proteger la información que su área maneja y custodia, por lo que deben tomar con la debida profesionalidad el presente documento y actuar de oficio ante cualquier transgresión en su área a la seguridad de la información.

C. Acceso a los equipos personales

A continuación ofrecemos una serie de aspectos por considerar y que deben ser acatados por el personal de la DGSC.

1. La adecuación final de los servicios y programas (software) será realizada por Soporte Técnico.
2. Soporte Técnico es custodio irrevocable de los manuales técnicos y medios que contengan los drivers, programas, sistemas, Sistemas Operativos y sistemas expertos y cualquier otro algoritmo o programación que se requieran para facultar los bienes informáticos como herramientas útiles para el depositario en el cumplimiento de sus deberes.
3. Los equipos personales asignados al personal de la DGSC es propiedad de la Dirección General de Servicio Civil, por lo que esta última es la encargada de decidir las aplicaciones de software que se pueden utilizar en la institución y cuales están restringidas. Normalmente esta decisión la tomarán los Directores de Área en conjunto con el Coordinador de UTIC.
4. El uso que se dé a los equipos personales de la DGSC debe ser exclusivamente en procura del cumplimiento de funciones del responsable y en paralelo a las metas de la institución.
5. Todo software instalado en los equipos personales debe estar aprobado por UTIC, quien es el único autorizado, mediante Soporte Técnico, de instalar cualquier aplicativo o código en los equipos.
6. De ser requerida la instalación de software que no sea propiedad de la DGSC, el usuario deberá justificar su uso y solicitar autorización a su jefatura inmediata, quien mediante un oficio informará a UTIC para su criterio y posterior instalación en el equipo o equipos designados y el periodo de tiempo que el software debe estar disponible.
7. Queda prohibida la instalación, almacenamiento o ejecución de software sin la respectiva licencia que faculte al usuario para dichos fines. De encontrar software en estas condiciones representa una falta grave, por lo que se desinstalará de inmediato y se informará al Director de área correspondiente y a Recursos Humanos sobre la falta para su consideración.
8. Queda prohibido guardar en los equipos información tal como música, videos, documentos, programas y archivos que no estén relacionados con el cumplimiento estricto de las labores asignadas al usuario del equipo.
9. Queda prohibido el realizar actos que puedan significar la infracción de leyes en los equipos personales, como por ejemplo infracciones a la autoría de investigaciones o documentos y productos, difamación, ataques informáticos y creación de spam.

10. Queda prohibido a los funcionarios de la DGSC el alterar o eliminar las configuraciones del equipo asignado.
11. Es responsabilidad del usuario el velar por que la información relevante contenida en su computadora personal esté debidamente respaldada, para evitar pérdida accidental de datos.
12. Los usuarios deben respaldar de manera periódica la información sensible que se encuentre en sus computadoras personales, pudiendo solicitar asesoría a UTIC sobre el tema.
13. Es responsabilidad de cada colaborador el solicitar a su respectivo superior la capacitación requerida para el manejo de las herramientas informáticas que se utilizarán en su equipo, para evitar el mal uso y maximizar el rendimiento de las aplicaciones.

D. Acceso a servidores

La administración, configuración y custodia de los servidores institucionales es tarea del equipo humano de UTIC, razón por la que se establecen las siguientes pautas a seguir:

1. El uso de los servidores y equipo de informática será exclusivo para apoyar las funciones y requerimientos de la DGSC. No podrá utilizarse con fines personales o fuera del contexto de servicio institucional.
2. Queda prohibido el realizar en los servidores acciones que puedan implicar infracciones a la ley.
3. El Administrador de Servidores será quien posea y resguarde los programas, sistemas, Sistemas Operativos, software, licencias, actualizaciones y ejecutables requeridos para asegurar que los servidores estarán óptimos para cumplir con su funciones.
4. Cuando el Administrador de Servidores o el Encargado de Telecomunicaciones detecten una falla en la función de

un equipo, deben informar inmediatamente al Coordinador de UTIC, para valorar si se posee garantía y su inmediata solicitud de cambio o reparación.

5. Cualquier falla en equipo de informática, ya sea por hardware o software, debe quedar anotada en la Memoria de Fallas de Servicios de la DGSC.

6. Es obligación del Administrador de Servidores el monitorear constantemente la función de los servidores y su efectiva prestación de servicio.

7. Es obligación del Administrador de Servidores el implementar y ejecutar un esquema estricto de copias de respaldo y procedimientos de recuperación de la información que el Coordinador de UTIC considere crítica.

8. Es obligación del Encargado de Telecomunicaciones el monitorear constantemente la función de la red y su efectiva prestación de servicio.

E. Acceso a servicios

El acceso a los recursos informáticos y servicios que provee la Dirección General de Servicio Civil, tales como correo electrónico institucional, Internet, servicios de red y dominio es suministrado a los empleados de la DGSC como soporte para la óptima realización de sus actividades. Es por eso que todo uso que se de a estos recursos debe considerar:

1. Todo uso de los recursos informáticos de la DGSC está sujeto a cumplir con las normas y restricciones aquí expuestas. El usuario debe asegurar que el uso a estos recursos sea preciso, apropiado, ético y direccionado al logro de los objetivos de la DGSC.
2. Aquellos recursos informáticos que sean dotados al personal de la DGSC por la organización son propiedad de la misma. Por ello, la DGSC monitorea y toma las medidas que se consideren pertinentes para verificar el correcto uso de los recursos y la protección a la calidad de los mismos.

3. UTIC está en obligación de avisar por medios oficiales cuando se vaya a realizar la suspensión de un servicio por mantenimiento o por fuerza mayor, inclusive cuando se trate de causas que no estén en las manos de UTIC dada la naturaleza de la suspensión, a efecto de mantener información precisa sobre estas situaciones y evitar interpretaciones inadecuadas o imprecisas.

F. Acceso a Internet

Todos los servicios y recursos informáticos dotados por la DGSC para sus colaboradores son un apoyo para el logro de sus encomiendas profesionales, según su cargo y responsabilidades, por lo que el uso del servicio institucional de Internet queda sujeto a la consecución de objetivos de la DGSC y encomiendas directas profesionales. El uso de Internet para acceder, publicar, publicitar, manipular u obtener contenido que vaya en contra de los valores institucionales, que pueda ser considerado discriminatorio, ofensivo, obsceno, sexual, destructivo o amenazante para la moral, la institución, el gobierno o la patria está absolutamente prohibido.

El servicio de Internet institucional debe ser utilizado exclusivamente para fines congruentes con los objetivos de la DGSC como lo son la investigación, desarrollo, consulta, referencia y comunicación.

Es deber de la UTIC solicitar e implementar los equipos y métodos que se consideren pertinentes para impedir el acceso a sitios que no sean compatibles con las necesidades de la DGSC.

Cuando algún usuario de Internet institucional requiera el acceso a un sitio que este bloqueado por la seguridad implementada por la UTIC, debe presentar una solicitud al Coordinador de UTIC avalada por el Director de su área para que se garantice su acceso al sitio.

Todo el personal de la DGSC tiene derecho a acceder al servicio de Internet institucional.

Está restringido el uso de programas de chateo sin la autorización del señor Director General y su comunicación al Coordinador de UTIC.

Está restringido el uso de Internet para obtener y bajar música, videos y ejecutables que no estén relacionados con

las funciones desempeñadas en la DGSC y la consecución de los objetivos institucionales.

Será considerado como un ataque a la seguridad informática de la DGSC cualquier acción no autorizada, sea interna o externa, que resulte en una exploración de características, detalles y vulnerabilidades de las tecnologías de comunicación de la infraestructura de la DGSC.

El personal de la DGSC no debe establecer ni configurar conexiones locales o remotas, ya sean internas o externas con otros equipos utilizando, sin autorización explícita de la UTIC, la infraestructura de telecomunicaciones de la Dirección General de Servicio Civil.

La Dirección General de Servicio Civil procurará brindarles a los visitantes un servicio de Internet de calidad, con las restricciones y limitaciones pertinentes para asegurar que este servicio no se convierta en un portal para ciberataques. Es por ello que cualquier visitante que requiera el acceso a Internet debe hacer la solicitud, ya sea personal o por medio de un contacto de la DGSC, a UTIC para la creación del usuario y contraseña temporal, que en ningún caso debe superar 1 día, salvo casos de excepción debidamente justificados por la Autoridad Institucional competente para ello. El visitante al ser atendido debe quedar inscrito en la Bitácora de Uso de la Red de Invitados y se debe implementar rastreo y seguimiento de actividad para futuras evaluaciones. De detectarse un comportamiento transgresor se le incluirá en la Lista de Negación de Servicios de Informáticos con las pruebas del caso y no se le volverá a permitir el acceso a los servicios informáticos de la DGSC.

G. Acceso a administración de equipos de comunicación y seguridad

Es deber de UTIC el administrar los equipos de comunicación y de seguridad. Específicamente es deber del Encargado de Telecomunicaciones el velar por el funcionamiento correcto y oportuno de la red LAN de la DGSC. Además, debe realizar pruebas periódicas y mantenimientos para asegurar el funcionamiento de la red LAN, así como que el total de sus capacidades esté disponible para el uso institucional.

La UTIC está habilitada para realizar monitoreos de equipos, sistemas y tráfico de red en cualquier momento que se considere necesario para corroborar la seguridad de la información y el correcto funcionamiento de las redes y servicios.

Queda prohibido el utilizar cualquier herramienta o mecanismo de monitoreo de tráfico de red o de sistemas sin previa autorización del Coordinador de UTIC.

Se prohíbe realizar pruebas de debilidades de seguridad sin la autorización de la jefatura de UTIC y las mismas deberán solamente ser realizadas por el personal autorizado en un ambiente controlado previa autorización del Coordinador de UTIC

H. Sobre el uso del servicio de correo institucional

Con el propósito de velar por el funcionamiento efectivo y correcto del correo institucional, se establecen los siguientes puntos a seguir:

1. Para acceder al correo institucional el usuario debe contar con usuario de dominio, lo que implica lo estipulado para tales efectos en el apartado A. del presente apartado.
2. Todos los servicios y recursos informáticos dotados por la DGSC para sus empleados son un apoyo para el logro de sus encomiendas administrativas, técnicas o profesionales, según su cargo y responsabilidades, por lo que el uso del correo electrónico institucional queda sujeto a enviar y recibir mensajes relacionados con sus funciones y objetivos de la DGSC.
3. Revisar el correo electrónico es de carácter obligatorio y se considera un medio oficial de comunicación institucional.
4. Las cuentas de correo son personales y no son transferibles. El usuario propietario de la cuenta es el único responsable final de la privacidad de su contraseña y el uso que se dé a su cuenta. Cualquier uso contrario a lo aquí dispuesto para las cuentas de correo será imputado al propietario.

5. Todo envío de correo masivo que se requiera realizar debe ser notificado con una semana de antelación a UTIC para su autorización.

6. El abrir adjuntos de correo siempre supone un riesgo de seguridad. Es responsabilidad del usuario el valorar quien le envía el correo y el riesgo de ejecutar o abrir el adjunto.

7. La creación de las cuentas de dominio y correo electrónico son responsabilidad única y exclusiva de UTIC, siempre atendiendo la petición de Recursos Humanos o en aquellos casos donde por algún mantenimiento o sistema se requiera.

8. Queda prohibido el uso del servicio institucional de correo para enviar mensajes que atenten contra el orden, contra la dignidad humana o las garantías y derechos fundamentales.

9. Queda prohibido el uso del servicio institucional de correo para enviar mensajes con fines personales, publicitarios, comerciales o religiosos.

10. Queda prohibido el uso del servicio institucional de correo para enviar adjuntos que resulten peligrosos o atenten contra la seguridad de la información.

11. Es obligación de cada usuario del servicio institucional de correo el resguardar su información (pst)

I. Sobre el acceso al código fuente de las aplicaciones de la DGSC

Con la finalidad de resguardar los sistemas informáticos que desarrolla la DGSC, es obligación de la UTIC respaldar interna y externamente el código fuente de todos los sistemas de información desarrollados por cada miembro de la unidad de informática.

Por tal motivo se debe contar con un repositorio central (en las instalaciones de la DGSC) con el código fuente de todos los sistemas informáticos para su consulta o atención

y elaborar semanal o mensualmente una copia de respaldo que ha de almacenarse fuera de la institución.

Las actualizaciones al código fuente sea por nuevas mejoras o ajustes debe ser tarea asignada a una sola persona evitando así la posibilidad de errores debido a la manipulación de varios profesionales de la UTIC los cuales involuntariamente pueden generar versiones erróneas del código fuente.

IV. COMPROMISO DEL RECURSO HUMANO CON LA SEGURIDAD DE LA INFORMACIÓN

Política

Todo el personal de la Dirección General de Servicio Civil debe tener conocimiento y aceptación de las condiciones de confidencialidad, uso adecuado de los recursos informáticos, los datos y la información propiedad de la DGSC o que haya sido entregada en calidad de custodia por el usuario para que la institución la salvaguarde según la Ley N° 8968 (Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales). Así como el estricto cumplimiento de lo expuesto en el "Documento Integral de Seguridad de la Información de la DGSC".

Obligaciones

Es responsabilidad del personal de la Dirección General de Servicio Civil cumplir estrictamente lo establecido en el Documento Integral de Seguridad de la Información de la DGSC y las leyes aplicables al trato de información a la cual se encuentre sometida la DGSC y su personal.

V. SANCIONES

Cualquier violación a lo dispuesto en este documento deberá ser sancionada según el daño y el riesgo para la integridad de la información. Las sanciones pueden incluir,

sin detrimento a otras posibilidades, una sanción por escrito con copia al expediente, el retiro del equipo informático, la suspensión del servicio o una sanción económica para resarcir el daño al estado.

El personal de la DGSC que no cumpla con lo expresado en este documento en razón de la protección de la información, el uso de su cuenta de dominio y las claves bajo su custodia se expone a las siguientes sanciones:

- a. En la primera incidencia se le solicitará al jefe inmediato la amonestación verbal y la cuantificación de las infracciones.
- b. En la segunda incidencia se le dirigirá una amonestación por escrito con copia a su expediente y su superior inmediato, indicando las fallas.
- c. En la tercera incidencia se le retirará el bien y/o servicio, notificando por escrito al jefe inmediato y al usuario infractor las razones del retiro.
- d. Las sanciones económicas serán definidas por Recursos Humanos, Coordinador de UTIC y Asesoría Jurídica en reunión, basándose en el criterio emitido previamente por UTIC.

Todas las acciones que no estén descritas en este documento pero que sin embargo comprometan la seguridad e integridad de la información deberán ser revisadas por la UTIC, quien emitirá un criterio técnico para ser considerado.

VI. CONTINUIDAD DE LOS SERVICIOS

A. Generalidades

La UTIC debe poseer una definición de roles detallada, donde se especifiquen las tareas para cada rol y su función en el Equipo de Recuperación de Desastres. Cada área de la DGSC debe tener un manual de operaciones propio para afrontar desastres informáticos. Además se deben realizar simulacros o pruebas periódicas de la efectividad y validez de los planes de contingencia, manuales y tiempos de respuesta. Por último, los Manuales de Recuperación

de Servicio deben actualizarse en respuesta a toda actualización tecnológica de la estructura de la DGSC.

B. Respaldo de datos

Es responsabilidad directa de la UTIC definir un profesional que desempeñe las funciones de Administrador de Base de Datos.

Dentro de sus funciones esta la elaboración de planes de respaldo y restauración de base de datos en ambientes controlados garantizando la ejecución de dichas labores de forma efectiva y ágil.

La DGSC debe velar por la capacitación adecuada para dicho profesional buscando los convenios necesarios que garanticen la adquisición de dicho conocimientos o bien reservando las partidas presupuestarias para la capacitación del personal asignado.

Dentro de sus funciones se contemplan las siguientes:

1. El Administrador de Bases de Datos será el encargado de coordinar junto al Administrador de Servidores la tecnología a utilizar (software y hardware) para realizar los respaldos de la información considerada sensible de la DGSC.
2. El Coordinador de la UTIC es responsable de determinar qué información es sensible y candidata para ser incluida en los respaldos periódicos de información. Para ello podrá consultar y reunirse con quien considere necesario para detectar efectivamente la información crucial.
3. El Coordinador de la UTIC junto al Administrador de Bases de Datos y el Administrador de Servidores categorizarán la información sensible a respaldar según su criticidad y conveniencia, para así determinar la periodicidad de los respaldos por categoría, según lo dispuesto en el Índice de Respaldo de la Información.
4. El Administrador de Bases de Datos es el encargado de realizar los respaldos correspondientes de la información y llevar un orden de recursos. Es además el encargado de realizar las restauraciones. En su ausencia,

el Administrador de Servidores podrá realizar estas funciones.

5. Se debe adquirir un servicio de almacenaje de medios de un tercero, que garantice la seguridad, oportunidad, confiabilidad y exactitud de la información contenida en los medios. Con una respuesta no mayor a 4 horas para devolver un medio en caso de una catástrofe.

C. Manuales de instalación de los servicios institucionales

La UTIC, mediante sus especialistas, debe adquirir o producir manuales efectivos que lleven a la recuperación de los servicios informáticos y la información en el menor tiempo posible y con la mayor calidad.

Se deben contar con al menos los siguientes manuales, los cuales estarán a disposición de los funcionarios de UTIC en caso de que el encargado de cada área no pueda enfrentar directamente la situación:

- a. Manual de Recuperación del Servicio de Active Directory y dominio.
- b. Manual de Recuperación del servicio Exchange (correo institucional)
- c. Manual de Recuperación de Sistema de Gestión de Bases de Datos y de la información de esquemas
- d. Manual de Recuperación de Equipos de Seguridad.
- e. Manual de Recuperación de Máquinas Virtuales.
- f. Manual de Recuperación de Servidor de Archivos.
- g. Manual de Recuperación del Sitio Web
- h. Manual de Recuperación de Sistemas de la DGSC
- i. Manual de Recuperación de Servicios de Telecomunicación
- j. Manual de Recuperación de Equipos Personales
- k. Manual de Recuperación de Antivirus institucional
- l. Manual de recuperación de interfaces externas a otros sistemas

Los manuales detallados en el punto anterior deben mantenerse actualizados acorde con la realidad tecnológica de la DGSC.

D. Capacitación

Todo el recurso humano de la Dirección General de Servicio Civil debe contar con una inducción por parte de funcionarios de la UTIC sobre el presente documento y las obligaciones que conciernen al funcionario. Además, UTIC en conjunto con Recursos Humanos planificará una capacitación anual en Seguridad Informática Básica a los recursos de reciente ingreso impartida por funcionarios de la UTIC.

La DGSC está en la obligación de facilitar la capacitación al personal de la UTIC al menos en áreas tales como:

- Seguridad Informática
- Gestión de Bases de Datos
- Administración de Servidores
- Buenas prácticas de gestión informática (ITIL)
- Administración de Redes

El Coordinador de UTIC será el responsable de buscar y planificar dicha capacitación y la DGSC facilitará los recursos mediante planificación conjunta para realizar dicho esquema, que se planteará anualmente.



DIRECCIÓN GENERAL DE SERVICIO CIVIL

"Contribuyendo a la Gobernabilidad Democrática de Costa Rica desde 1953"

San Francisco de Dos Ríos,
125 metros este del templo católico.

Central telefónica (506) 2586-8300
Apartado Postal 3177-1000 SJ
www.dgsc.go.cr
San José, Costa Rica