MEMORANDO

DGA-0056-2025

PARA: Personal de la Contraloría General de la República

DE: Manuel Martínez Sequeira, Gerente
División de Gestión de Apoyo

ASUNTO: Actualización de Lineamientos de Seguridad de la información

FECHA: 23 de junio de 2025

Nos permitimos hacer del conocimiento general que mediante resolución número R-DC-00069-2025 de las catorce horas del veinte de junio de dos mil veinticinco, el Despacho Contralor emitió las nuevas Directrices de Seguridad de la Información. Estas se ajustan a lo dispuesto en la norma ISO/IEC 27001 en su última versión del año dos mil veintidós, la principal norma a nivel mundial que regula la gestión de la seguridad de la información.

Consecuentes con lo anterior, esta Gerencia de División emite y comunica, por este medio, los nuevos Lineamientos de Seguridad de la Información, los cuales responden a las directrices previamente señaladas.

Estos nuevos lineamientos no solo actualizan el marco interno a la norma ISO/IEC 27001:2022, sino que también incorporan nuevas secciones y controles para fortalecer la confidencialidad, integridad y disponibilidad de la información institucional.

Ambos documentos establecen las consideraciones de seguridad que en adelante deberán ser tomadas en cuenta por el personal para hacer un uso adecuado de la información que se gestiona como parte de los procesos institucionales. Por lo tanto, recomendamos su lectura y aplicación obligatoria.

Podrán consultar las nuevas Directrices de Seguridad de la Información y los Lineamientos de Seguridad de la Información en la Intranet institucional, en la sección Documentos Marco normativo de Seguridad Información.

CGR Firmado digitalmente
Valide las firmas digitales

MMS/MAZM/gab
G: 2025000421-1
C: 2025013647

LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

División de Gestión de Apoyo

Versión	Asunto	Fecha
1.0	Primera versión de los lineamientos	01 de agosto, 2019
1.1	Ajustes en redacción y cambios menores	16 de enero, 2020
1.2	Lineamiento sobre plataformas de procesamiento analítico	11 de noviembre, 2020
1.3	Lineamiento sobre desvinculación o desasociación de datos personales	08 de agosto, 2023
2.0	Alineamiento de lineamientos con la ISO 27001:2022	23 de junio, 2025

Junio, 2025

Contraloría General de la República
T: (506) 2501-8000, C: contraloria.general@cgrcr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

ÍNDICE GENERAL

A. Introducción

El presente documento establece los lineamientos derivados de las directrices de seguridad de la información de la Contraloría General de la República (CGR).

El documento adopta como orientación y buena práctica internacional aceptada, la norma ISO 27001:2022 “Seguridad de la información, ciberseguridad y protección de la privacidad – Controles de seguridad de la información”. Esta norma sugiere la creación de una serie de documentos normativos, tales como políticas, directrices, lineamientos, guías y controles, con el objetivo de dirigir las medidas de seguridad de la información relacionadas con la institución, y adaptadas en el contexto de la nueva modalidad de trabajo híbrido.

B. Objetivo

Establecer una orientación interna derivada de las directrices de seguridad de la información vigentes de la CGR, que sirva como instrumento para el personal en el uso seguro de la información gestionada por la Institución, como parte de las funciones asignadas por ley.

C. Alcance

Los presentes lineamientos son de acatamiento obligatorio para el personal de la CGR, conforme lo dispuesto en el apartado II de la resolución R-DC-000069-2025 de las Directrices de Seguridad de la Información.

D. Compromiso Institucional

Conforme con las Directrices de Seguridad de la Información:

> *La CGR implementará un sistema de gestión de seguridad de la información (SGSI), que permita identificar y minimizar los riesgos a los cuales se expone la información. Además buscará desarrollar una cultura interna que promueva su protección y garantice el cumplimiento de los requerimientos legales. Dicho modelo se sustentará tanto en la política 33 de Buen Gobierno Corporativo, como en las directrices de seguridad formuladas en el presente documento y que están orientadas a dirigir la aplicación específica de esa política.*
> *Para la implementación del SGSI, se deberá definir como punto de partida la criticidad y la confidencialidad de la información institucional, de manera tal que los esfuerzos en materia de aseguramiento de la información, estén alineados con*

estas características. En consecuencia, el proceso de aseguramiento de la información deberá responder a lo que la administración defina como crítico o confidencial.
El Despacho Contralor, con la asesoría del Comité de Gobierno de las Tecnologías de Información y Comunicaciones (CGTIC) y del CISO, promoverá el establecimiento y operación de la plataforma de seguridad tecnológica, atendiendo aquellos requerimientos propuestos por la Unidad de Tecnologías de Información (UTI). *Dada la importancia de su rol dentro de la construcción, levantamiento y sostenibilidad del SGSI, el CISO deberá de contar con los recursos necesarios para cumplir con este compromiso. Para ello, y en la medida de las posibilidades, se buscará dotar de recursos adecuados para implementar y mantener el marco de seguridad definido y verificar su cumplimiento.*

Por este motivo y en virtud de la dependencia y relación existente de los lineamientos a la correspondiente directriz, el compromiso indicado en las directrices se conserva en los respectivos lineamientos indicados en este documento.

Es responsabilidad del jerarca y de los titulares subordinados promover en el personal, el conocimiento y acatamiento de los presentes lineamientos de seguridad de la información.

E. Controles organizacionales

E.1 Roles y responsabilidades de seguridad de la información

E.1.1 Despacho Contralor

E.1.1 El Despacho Contralor define la estrategia global de seguridad de la información, alineada con la estrategia institucional y las Directrices de Seguridad de la Información. Además, aprueba las directrices y lineamientos relacionados con la seguridad de la información y asigna los recursos necesarios para el funcionamiento del Sistema de Gestión de Seguridad de la Información (SGSI).

E.1.2 Oficial de Seguridad de la Información (CISO)

E.1.1.1 El Oficial de Seguridad de la Información (CISO) será el líder institucional en materia de seguridad de la información.

E.1.1.2 Cuando se presente un incidente de seguridad de la información, se activará el Equipo de Respuesta a Incidentes de Seguridad de la Información (CSIRT), el cual estará liderado por el CISO y coordinará todos los esfuerzos para la contención, erradicación, recuperación y análisis del incidente, así como la gestión de la comunicación y el aprendizaje derivado del evento.

E.1.1.3 El CISO dependerá funcionalmente de la Gerencia de la División de Gestión de Apoyo.

E.1.1.4 Para lo que corresponde en materia de seguridad documental, el CISO se apoyará en un representante de la USI, que actuará como enlace y colaborador en la definición, implementación y control de las medidas de seguridad aplicables a la información documental.

E.1.1.5 Para lo que corresponde a materia de seguridad física, el CISO se apoyará en un representante de la USG.

E.1.1.6 Para lo que corresponde a ciberseguridad, el CISO mantendrá una estrecha coordinación con el equipo de la UTI responsable de la ciberseguridad de las TIC, estableciendo canales de comunicación fluidos y mecanismos de colaboración que permitan una respuesta coordinada ante amenazas y vulnerabilidades, así como la correcta aplicación de las políticas y controles de seguridad en el ámbito tecnológico.[1]

E.1.1.7 El CISO tendrá las siguientes funciones:

Función	Coordina con Gerente DGA	Gestiona que se haga	Responsable de hacerla
Definir, implementar y mantener actualizadas las directrices, lineamientos y guías en materia de seguridad de la información de la CGR.	**X**		**X**
Realizar procesos de validación para garantizar la adecuada aplicación de las orientaciones internas de seguridad de la información, por parte del personal.			**X**
Realizar campañas de sensibilización para todo el personal en materia de seguridad de la información.			**X**
Participar en los procesos de inducción del nuevo personal con el tema de la seguridad			**X**

[1] Se refiere a redes, servidores, ciberseguridad, telefonía, estaciones de trabajo, IoT y sistemas de información.

Función	Coordina con Gerente DGA	Gestiona que se haga	Responsable de hacerla
de la información.			
Monitorear el entorno externo de la seguridad para determinar posibles riesgos que pueda enfrentar la información institucional.		**X**	**X**
Coordinar con las unidades responsables dentro de la CGR la identificación, análisis y evaluación de riesgos de seguridad de la información, así como la implementación de medidas de prevención, mitigación y respuesta ante incidentes.		**x**	**x**
Supervisar y analizar las bitácoras de los dispositivos de seguridad para identificar eventos sospechosos, patrones anómalos y posibles incidentes de seguridad, y coordinar con la UTI la implementación de acciones de mitigación y respuesta oportuna.		**X**	**X**
Gestionar e instruir al personal de la UTI responsable la aplicación de medidas correctivas respecto a vulnerabilidades detectadas sobre la información, considerando los tres pilares de la seguridad: Información digital, documental o sobre instalaciones donde se procese, almacene o genere información.	**X**	**X**	
Supervisar y asegurar el funcionamiento continuo y la mejora del Sistema de Gestión de Seguridad de la Información (SGSI) institucional.	**X**		**X**
Asesorar a la Gerencia de la DGA en la toma de decisiones estratégicas y administrativas relacionadas con la seguridad de la información.			**X**

Función	Coordina con Gerente DGA	Gestiona que se haga	Responsable de hacerla
Participar con la Gerencia de la DGA en la atención de requerimientos en materia de planificación, presupuesto y demás proyectos institucionales relacionados con la seguridad de la información.	**X**		**X**
Velar por la ejecución de los procesos de gestión de vulnerabilidades, gestión de actualizaciones y gestión de cambios por parte de la UTI.		**X**	
Asesorar a la Gerencia de la DGA sobre la necesidad de realizar estudios de auditoría externa o solicitar apoyo de la auditoría interna para evaluar la eficacia del SGSI.	**X**	**X**	
Realizar investigaciones específicas de temas asociados al área de la seguridad de la información para promover la aplicación de nuevas estrategias de seguridad.			**X**
Supervisar la gestión del riesgo en seguridad de la información.		**X**	**X**
Desarrollar y mantener una estrategia de seguridad de la información que esté alineada con la estrategia, objetivos y necesidades del negocio.	**X**		**X**
Rendir cuentas al Gerente de la DGA respecto de los asuntos atendidos.	**X**		**X**
Participar activamente en los proyectos donde se requiera garantizar un alineamiento con la política de seguridad.			**X**
Liderar y coordinar el grupo de respuesta a incidentes de seguridad de la información (CSIRT)			**X**

E.1.1.8 El CISO mantendrá comunicación con instituciones externas, tanto nacionales

como internacionales, relacionadas con la seguridad de la información, que se encarguen de monitorear el entorno y emitan alertas respecto a riesgos de seguridad detectados y, con base en estas alertas, coordinará con los responsables de las unidades necesarias dentro de la CGR la aplicación de medidas preventivas y/o correctivas con el fin de mitigar los riesgos asociados a las alertas recibidas.

E.1.1.9 El CISO deberá documentar todas las acciones, recomendaciones y decisiones tomadas en respuesta a alertas o comunicados externos recibidos de instituciones relacionadas con la seguridad de la información, incluyendo las alertas y comunicados provenientes de servicios de monitoreo de seguridad.

E.1.1.10 El CISO implementará un proceso de inteligencia de amenazas que le permita recopilar, analizar y evaluar información relevante sobre amenazas a la seguridad de la información, con el objetivo de obtener una visión integral del panorama de riesgos, comprender las tendencias y tácticas de los actores maliciosos y generar conocimiento que permita a la CGR anticiparse a las amenazas.

E.1.1.11 El CISO deberá realizar un monitoreo en foros y publicaciones técnicas, en orden a verificar de manera continuada, la robustez y seguridad de los modelos y sistemas de Inteligencia Artificial (IA) en uso por parte de la CGR, verificando que sean ciberseguros, funcionen según lo previsto y también sean resistentes a ser comprometidos por partes no autorizadas, ni se ponga en riesgo la seguridad de los usuarios y la confidencialidad de la información institucional.

E.1.3 Equipo de Respuesta a Incidentes de Seguridad de la Información (CSIRT)

E.3.1 El CSIRT, será un equipo conformado por personal designado para atender el tema de los incidentes de seguridad de la información a nivel Institucional.

E.3.2 El CSIRT será convocado por el CISO en el momento en que se presente un incidente y permanecerá activo durante todo el tiempo que dure su atención.

E.3.3 El CSIRT estará conformado por:

- El CISO, quien liderará y coordinará la respuesta a incidentes.
- El coordinador del área de infraestructura de la UTI, como responsable técnico.
- Un representante de la USG, experto en seguridad física.
- Un representante de la USI, experto en seguridad documental.

- Otros miembros del personal, según la naturaleza del incidente, como personal legal, de comunicaciones, o de gestión del recurso humano.

E.3.4 El CSIRT se reunirá de forma periódica, al menos dos veces al año, para revisar y actualizar los procedimientos de gestión de incidentes, evaluar la efectividad de la respuesta a incidentes previos, identificar áreas de mejora y fortalecer la preparación del equipo ante posibles eventos futuros. El CISO podrá convocar reuniones adicionales cuando lo considere necesario, por ejemplo, tras la ocurrencia de un incidente relevante o ante cambios significativos en el entorno de la seguridad.

E.1.4 Unidad de Tecnologías de la Información (UTI)

E.1.4.1 La UTI es responsable de implementar y mantener la plataforma de seguridad tecnológica. Esto abarca, entre otras funciones, la gestión de la infraestructura tecnológica, la aplicación de controles de software y hardware, la administración de accesos y la gestión de vulnerabilidades, asegurando la protección de la información y el cumplimiento de las políticas de seguridad de la CGR.

E.2 Inventario de información

E.2.1 El jerarca y titulares subordinados son los responsables de gestionar un inventario completo de toda la información institucional y clasificarla en función de su criticidad y confidencialidad, mediante un Modelo de Arquitectura de Información (MAI), en alineamiento con la estructura del MAGEFI. Para asegurar esta alineación, el jerarca y los titulares subordinados deberán trabajar en conjunto con la UGC, quien es la encargada del MAGEFI.

E.2.2 El CISO deberá participar de este proceso con el fin de apoyar en la definición de la información de acceso restringido, todo de conformidad con las directrices institucionales para el manejo de información de acceso restringido en la CGR, resolución R-DC-75-2017.

E.2.3 El MAI deberá incluir una clasificación clara y precisa de la información institucional pública, sensible y de acceso restringido, esta última considerando lo establecido por la resolución R-DC-75-2017 de directrices para el manejo de información de acceso restringido en la CGR.

E.2.4 Cualquier cambio en la clasificación de la información, o la incorporación de nuevos insumos o productos a la documentación de un proceso o procedimiento del MAGEFI, es responsabilidad de los dueños de la misma, así como actualizar el sistema con el fin de mantener al día la información del MAI, previa coordinación con la UGC en materia de la base de datos sobre el MAGEFI.

E.2.5 Este proceso de clasificación deberá revisarse al menos una vez al año con el propósito de mantener la información actualizada y vigente. Esta revisión será liderada por la UGC en conjunto con los dueños de los procesos.

E.3 Clasificación y manejo de la información

E.3.1 Protección de datos personales

E.3.1.1 La información que contenga datos personales debe ser identificada, protegida y despersonalizada cuando sea necesario, de acuerdo con las orientaciones internas de la CGR, y cumplir con los requisitos que establece la Ley de Protección de la Persona frente al tratamiento de sus datos personales nº 8968 y su reglamento.

E.3.1.2 La despersonalización se aplicará a los datos personales que puedan afectar a su titular o los datos de acceso restringido o sensibles que consten en los productos documentales emitidos por las unidades orgánicas institucionales o los datos personales que sean custodiados en las bases de datos de la Contraloría General de la República.

E.3.1.3 Tratándose de información contenida en bases de datos institucionales, se atenderán las solicitudes que de manera formal realice la persona interesada titular de los datos, o por quien demuestre tener legitimación para ello, siempre que la solicitud cumpla con los requisitos señalados en el reglamento a la Ley nro. 8968. En tal caso, la despersonalización la realizará la unidad orgánica que administra la base de datos que contenga los datos a despersonalizar.

E.3.1.4 En el caso de productos documentales nuevos que contengan información sensible o de acceso restringido, se deberá generar una versión despersonalizada en el momento de su emisión. Esta versión despersonalizada se utilizará para fines de consulta o divulgación, mientras que la versión original con los datos completos se conservará de forma segura y confidencial, de acuerdo con las políticas de seguridad de la información.

E.3.1.5 La UTI deberá establecer las herramientas tecnológicas y protocolos para despersonalizar los datos, en documentos y en sistemas de información, según sea requerido por la unidad orgánica que administra la base de datos que contenga los datos a despersonalizar.

E.3.2 Manejo de información de acceso restringido

E.3.2.1 La clasificación de la información de acceso restringido será responsabilidad de los líderes funcionales, en ejercicio de su competencia, y se formalizará mediante las orientaciones internas que se establezcan en la CGR. Esta clasificación deberá ser

revisada y actualizada periódicamente para asegurar su pertinencia y adecuación a las necesidades de la CGR.

E.3.2.2 Toda información clasificada de acceso restringido, independientemente del formato (digital, físico), deberá estar claramente identificada como tal.

E.3.2.3 Los líderes de los procesos en los cuales se maneje información de acceso restringido, deberán identificar los puntos donde esta información es manipulada, ya sea que se recopile, transmita, almacene o elimine, no importando si la información se encuentra en formato físico o digital.

E.3.2.4 Los responsables de los procesos que involucran información de acceso restringido, basados en lo establecido en las directrices y lineamientos de seguridad y cualquier orientación específica que el CISO haya definido, deberán definir los controles que procuren su seguridad para cada uno de los puntos donde es manipulada.

E.3.2.5 Todo el personal deberá firmar un acuerdo de confidencialidad, el cual detallará las responsabilidades del funcionario en cuanto a la protección de la información confidencial, las consecuencias de su incumplimiento y la duración de sus obligaciones de confidencialidad, incluso después de finalizada su relación laboral con la CGR.

E.3.2.6 La UGPH será la responsable de establecer los procedimientos para la gestión de estos acuerdos, incluyendo su formato, contenido, proceso de firma, almacenamiento seguro y seguimiento periódico. La UGPH también deberá garantizar que todo el personal esté debidamente informado sobre sus responsabilidades de confidencialidad y que se realicen actualizaciones o renovaciones periódicas de los acuerdos, según sea necesario.

E.3.2.7 La información de acceso restringido que sea almacenada en la nube debe cumplir con los controles de seguridad establecidos en este documento.

E.3.2.8 No se permite almacenar información de acceso restringido en aplicaciones gratuitas en la nube donde no exista un acuerdo de servicio (SLA) o una cláusula de confidencialidad, que garantice la seguridad, confidencialidad e integridad de la misma.

E.3.2.9 Todo el personal deberá acatar la prohibición de divulgar información de acceso restringido ante terceras personas.

E.3.2.10 Todo contrato con proveedores que implique el acceso o manejo de información de

acceso restringido, deberá establecer un acuerdo de confidencialidad con este proveedor garantizando la seguridad de la información gestionada como parte de la contratación.

E.3.2.11 La eliminación de información de acceso restringido debe ser realizada por el responsable de la información, y deberá garantizar el uso de algún mecanismo de borrado o destrucción segura de la información[2], dejando un registro documentado del proceso efectuado. Este proceso debe realizarse validando cualquier regulación que respalde esta información y si la misma está sujeta a la Ley del Sistema Nacional de Archivos.

E.3.2.12 En caso de detectar un incidente de seguridad que involucre información de acceso restringido, se debe activar el protocolo de gestión de incidentes de seguridad de la información. Se debe notificar inmediatamente al Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) institucional, quien se encargará de gestionar el incidente de acuerdo con los procedimientos establecidos, incluyendo la contención, la erradicación, la recuperación y el análisis post-incidente.

E.3.2.13 La información catalogada de acceso restringido en formato digital no podrá ser manipulada en dispositivos que no manejen las condiciones de seguridad requeridas y definidas en las guías emitidas por el CISO.

E.3.2.14 Los responsables de la elaboración de los controles para el manejo de información de acceso restringido deben considerar las interacciones y el intercambio de información con entidades externas a la CGR. Se deben establecer mecanismos de control y acuerdos de confidencialidad para garantizar que dichas entidades también cumplan con los estándares de seguridad y protección de la información establecidos por la CGR. El CISO definirá un protocolo institucional que dirija y oriente el intercambio de información con entidades externas a la CGR, de manera que garantice a las partes involucradas, un manejo seguro y confiable de dicha información.

E.3.3 Comunicación y publicación de información institucional

E.3.3.1 El personal de la CGR que tenga acceso o interactúe con información institucional, independientemente de su rol o nivel jerárquico, es responsable de su correcta gestión, incluyendo el cumplimiento de las políticas de seguridad, confidencialidad y protección de datos.

[2] Según protocolo definido por la UTI y la USI.

E.3.3.2 El personal debe hacer un uso íntegro de la información sin sacar provecho del acceso que tenga y velar por la protección de la información bajo su responsabilidad directa o sobre la cual tenga acceso.

E.3.3.3 El personal debe reconocer el valor de la información como un activo crítico de la CGR y, por lo tanto, debe protegerla contra cualquier acceso, uso, divulgación, modificación, destrucción o interrupción no autorizada. Esto implica la aplicación de controles de acceso, incluyendo la correcta configuración de permisos en documentos compartidos a través de servicios en la nube, la intranet, internet y otros sistemas institucionales. Se debe asegurar que la información sea accesible únicamente a las personas autorizadas y que los permisos se revisen y actualicen periódicamente. durante todo el ciclo de vida de los datos.

E.3.3.4 La comunicación de información institucional debe realizarse a través de los canales oficiales y siguiendo los lineamientos establecidos por la CGR, para evitar el riesgo de exponer ante terceros, información confidencial de forma no controlada. Además, es fundamental custodiar la información sensible de manera adecuada y cumplir con la obligatoriedad de no divulgar su contenido sin autorización.

E.3.3.5 La publicación de información o la emisión de criterios en nombre de la CGR en redes sociales, foros, blogs o cualquier medio de comunicación electrónico está reservada exclusivamente al personal autorizado por el Despacho Contralor.

E.3.3.6 Toda publicación de información institucional en los sitios web de la CGR, debe realizarse conforme a los “Lineamientos para la administración de los sitios web de la Contraloría General de la República”.

E.3.3.7 La apertura de cualquier usuario de una red social oficial de la CGR deberá ser autorizada por el CGTIC. Esto incluye la creación de cuentas relacionadas con los dominios o subdominios de la CGR, así como cualquier servicio de atención de nuestra institución. Se deben establecer procedimientos para la creación, gestión y uso de dichas cuentas, y se deberán ligar a la cuenta de correo o usuario correspondiente a la Administración de Sitios Web de la CGR, a cargo de la Unidad de Servicios de Información (USI) o la que asigne el CGTIC según corresponda.

E.3.3.8 La Unidad de Prensa será responsable de definir la estrategia de comunicación en redes sociales y el sitio web de la CGR, así como de seleccionar el contenido que se publicará. La USI, en coordinación con la Unidad de Prensa, se encargará de la administración de las cuentas, la configuración técnica, la seguridad, diseño gráfico

y todo tipo de material que represente la CGR (productos, servicios que produce o emite), respetando lo dispuesto en el Libro Marca institucional.

E.3.4 Transferencia de información

E.3.4.1 Cuando la CGR requiera obtener información de otras instituciones, esta debe ser solicitada y recibida a través de canales de comunicación seguros y previamente establecidos, que cumplan con las normas de seguridad física y lógica necesarias para proteger la confidencialidad e integridad de la información.

E.3.4.2 La información que las instituciones externas deban transferir a la CGR deberá ser depositada en plataformas o sistemas designados por la UTI específicamente para este fin, que cumplan con los estándares de seguridad física y lógica necesarios para garantizar la integridad, confidencialidad y disponibilidad de la información. Estos sistemas deben contar con mecanismos de autenticación, control de acceso, cifrado de datos, asegurando que la información se transmita y almacene de forma segura y que solo sea accesible para el personal autorizado.

E.3.4.3 La dependencia administrativa que reciba bases de datos de una entidad externa debe documentar mediante los mecanismos que defina la UTI, el nivel de confidencialidad asignado a dicha información, la lista de funcionarios autorizados para acceder a ella, el plazo de conservación establecido y la finalidad para la cual se recopila. Esta documentación debe ser custodiada por la UTI para asegurar su correcta gestión.

E.4 Proyectos de TIC

E.4.1 Todo proyecto institucional que involucre o use las TIC debe ser desarrollado en coordinación con la UTI. Esto incluye la creación de cualquier aplicativo utilizando herramientas de usuario final, en la que se gestione alguna base de datos u hoja electrónica con datos y que involucre a varios usuarios.

E.4.2 Los proyectos de tecnologías de la información deben cumplir con las directrices establecidas en la Metodología para la Formulación y Gestión de Proyectos de TI vigente en la CGR, sin detrimento de otras orientaciones institucionales en materia de gobernanza y gestión de las TI, diseño organizacional, mejora continua, como gestión y control de proyectos que le resulten aplicables.

E.4.3 En todo proyecto de tecnologías de la información se debe integrar la seguridad de la información como un elemento fundamental desde las etapas iniciales. Se debe involucrar al CISO en las fases del proyecto que sean necesarias para garantizar la protección de la información y el cumplimiento de las políticas de seguridad de la

CGR.

E.4.4 Todo desarrollo de proyectos de TIC que se realice para la CGR, incluyendo sistemas de información, infraestructura tecnológica, plataformas de datos y proyectos de analitica de datos, debe estar alineado con la planificación estratégica y táctica institucional. Además, deben cumplir con las orientaciones internas emitidas por la CGR en materia de gobernanza de datos, seguridad de la información, y cualquier otra normativa aplicable.

E.4.5 Todo participante en un proyecto de TIC, debe conocer y acatar lo dispuesto en la Metodología para la Formulación y Gestión de Proyectos de TI, otras orientaciones internas que los complementen, así como en estos lineamientos de seguridad.

E.5 Seguridad de la información en la relación con los proveedores

E.5.1 Todo proveedor que tenga acceso a información de acceso restringido deberá cumplir con los lineamientos establecidos en este documento.

E.5.2 Todo acceso a activos tecnológicos por parte de proveedores externos debe ser autorizado previamente por personal de la CGR.

E.5.3 Todo contrato establecido entre la CGR y proveedores externos, que involucre activos de información debe estar respaldado por un acuerdo de nivel de servicios (SLA) o una cláusula de confidencialidad. El SLA o dicha cláusula debe ser monitoreado, revisado y actualizado periódicamente para asegurar su adecuación a las necesidades de la CGR y a los cambios en el entorno tecnológico.

E.6 Servicios en la nube

E.6.1 La UTI gestionará la aplicación de los acuerdos de nivel de servicio (SLA) o las cláusulas de confidencialidad, establecidos con los proveedores de servicios en la nube, asegurando que se cumplan los niveles de servicio, seguridad y disponibilidad acordados.

E.6.2 El contrato establecido con los proveedores de servicios en la nube debe considerar al menos los siguientes aspectos:

- La CGR deberá garantizar que el proveedor de servicios en la nube no utilizará la información almacenada para otros propósitos distintos a los establecidos por la institución.
- El proveedor de servicios en la nube debe garantizar que a pedido de la CGR, entregará cualquier dato propiedad de la CGR que sea requerido.
- El proveedor debe contar con certificaciones reconocidas internacionalmente en materia de seguridad, que demuestren su capacidad

para proteger la información de la CGR.

E.6.3 Todo servicio contratado en la nube debe considerar las condiciones de seguridad necesarias para contar con niveles apropiados de disponibilidad, integridad y confidencialidad de la información gestionada. La UTI es la responsable de velar por el cumplimiento de estas recomendaciones.

E.6.4 En los contratos de Infraestructura como Servicio (IaaS), donde se contrata el acceso a recursos de computación en la nube, la UTI debe verificar que el proveedor cumpla con las condiciones de seguridad establecidas en el acuerdo. Esto incluye la protección de la información, la disponibilidad de los servicios y el cumplimiento de las normativas de seguridad aplicables.

E.7 Gestión de incidentes de la seguridad de la información

E.7.1 La gestión de los incidentes de seguridad de la información estará a cargo del CISO, quien según la necesidad se hará apoyar por el equipo de respuesta a incidentes de seguridad de la información (CSIRT).

E.7.2 Se establecen cuatro niveles de clasificación para las situaciones que afectan o podrían afectar la seguridad de la información:

- **Evento:** Cualquier ocurrencia observable en un sistema o red que potencialmente pueda afectar su funcionamiento o seguridad, pero que no constituye una violación de la seguridad de la información ni causa un impacto negativo. Los eventos se monitorean y documentan, pero no activan el proceso de gestión de incidentes.

- **Incidente menor:** Situación o condición que afecta la confidencialidad, integridad o disponibilidad, pero su impacto es limitado y no compromete un servicio crítico de la CGR. Estos incidentes se gestionan a nivel local por los responsables del servicio, y no requieren la activación del CSIRT.

- **Incidente mayor:** Situación o condición que resulta en una violación o amenaza inminente de violación de la confidencialidad, integridad o disponibilidad de sistemas o información críticos de la CGR. Este tipo de incidente causa una interrupción significativa de las operaciones, compromete información de acceso restringido, o puede resultar en un daño considerable a la reputación o a los recursos de la CGR. Este tipo de incidente activa al CSIRT para su gestión y resolución.

- **Catástrofe:** Destrucción total o parcial de la infraestructura de TI que causa la interrupción de los servicios TIC, imposibilitando la operación normal de la

institución. En este caso, se activa el plan de recuperación ante desastres, y no el proceso de gestión de incidentes.

E.7.3 Los incidentes de seguridad de la información pueden tener un origen técnico o no técnico. Un incidente técnico involucra la falla o el mal uso de activos tecnológicos (hardware, software, redes) que comprometen la confidencialidad, integridad o disponibilidad de la información. Los incidentes no técnicos se refieren a eventos que no involucran directamente la tecnología, pero que aún así pueden resultar en la pérdida, divulgación no autorizada o daño a la información confidencial.

E.7.4 Los incidentes de seguridad, ya sean menores o mayores, pueden ser detectados por diversas fuentes, entre ellas:

- Personal de la CGR: Cualquier funcionario que identifique un evento o situación anómala que pueda comprometer la seguridad de la información.
- Gestores de la plataforma de seguridad de la UTI: A través del monitoreo de los sistemas de seguridad, la detección de intrusiones, el análisis de logs y otras herramientas de seguridad.
- CSIRT del MICITT: En caso de incidentes que afecten a la infraestructura nacional o que requieran la colaboración de este equipo especializado.
- Clientes externos de la CGR: Si detectan alguna anomalía en la información o los servicios que reciben de la institución.
- Proveedores externos con contratos de monitoreo: A través de servicios de seguridad gestionados o de monitoreo de seguridad como servicio SOC, que brindan alertas sobre posibles incidentes.

E.7.5 Todo el personal de la CGR deberá contar con la preparación y competencias necesarias para poder detectar cuando ocurre un incidente de seguridad y proceder a informar mediante un reporte al Sistema de Órdenes de Servicio (SOS) de la UTI.

E.7.6 Para mayor claridad se indican algunos ejemplos de sucesos y su clasificación:

Situación	Clasificación
Solicitud de instalación de software específico	**Evento**
Reinicio programado de un servidor	**Evento**
Infección de virus en un equipo	**Incidente menor**
Un funcionario reporta un correo electrónico sospechoso que	**Incidente menor**

Situación	Clasificación
parece ser phishing	
Se detecta un equipo sin candado de seguridad debidamente colocado y cerrado y es reportado por un funcionario	**Incidente menor**
Ataque cibernético a sistemas institucionales: Se vulnera la página institucional y se pone una imagen no deseada en la misma	**Incidente mayor**
Un ataque de ransomware cifra archivos críticos en los servidores de la CGR, impidiendo el acceso a la información y afectando la operación de servicios esenciales	**Incidente mayor**
Robo de información de acceso restringido almacenada en un ampo en el archivo institucional	**Incidente mayor**
Incendio en edificio principal y anexo	**Catástrofe**

E.7.7 Los eventos y los incidentes técnicos menores serán atendidos a través de la mesa de servicio de la UTI, por los responsables de su gestión, o quién el CISO determine, sin que para esto se requiera convocar al CSIRT.

E.7.8 Los incidentes técnicos mayores se canalizan a través de la mesa de servicio para que se atiendan por el CSIRT, y las personas adicionales que el CISO determine según el tipo de incidente.

E.7.9 Los incidentes no técnicos, sean estos menores o mayores, deberán ser canalizados directamente al CISO. El CISO coordinará con las dependencias necesarias y responsables para la atención oportuna de los incidentes menores y solo convocará al CSIRT en el caso de incidentes mayores.

E.7.10 Los incidentes tipo catástrofe serán atendidos por la Comisión de Continuidad del Servicio (CCS) de forma conjunta con el CSIRT.[3] La CCS se encargará de coordinar las acciones necesarias para garantizar la continuidad de la CGR, mientras que el CSIRT se centrará en contener y mitigar el impacto del incidente, así como en llevar a cabo el análisis forense y las investigaciones correspondientes

E.7.11 En caso de incidentes de seguridad de la información clasificados como

[3] Se requiere de un proceso de gestión de la continuidad del negocio para la adecuada gestión de los sucesos tipo catástrofe.

catástrofes, se operará bajo lo indicado en la guía correspondiente de atención de catástrofes del Plan de Recuperación de Desastres (DRP) y el Plan de Continuidad del Negocio (BCP).

E.7.12 La UTI será la responsable de calificar el incidente técnico reportado y comunicarlo a los encargados de la atención del mismo.

E.7.13 La UTI deberá desarrollar y mantener actualizado un protocolo para respuesta a incidentes técnicos (IRP) en donde se indique el procedimiento paso a paso para la atención de tales casos y se informe al CISO cuando se active dicho protocolo.

E.7.14 La USG debe desarrollar un IRP que detalle el procedimiento a seguir para la atención de incidentes de seguridad de la información no técnicos y se informe al CISO cuando se active dicho protocolo.

E.7.15 El CISO es responsable de revisar, validar y aprobar los IRP técnicos y no técnicos.

E.7.16 El CISO, en coordinación con el CSIRT, definirá y ejecutará procedimientos de validación de la funcionalidad de los protocolos de respuesta a incidentes, incluyendo la realización de simulacros periódicos, al menos dos veces al año.

E.7.17 Todos los incidentes de seguridad y simulacros deben quedar debidamente documentados.

E.7.18 El CISO debe realizar como parte de sus responsabilidades lo siguiente:

a. Definir un procedimiento cuando corresponda para activar el CSIRT.
b. Definir la ubicación donde opera el CSIRT tanto para incidentes técnicos como no técnicos.
c. Mantener actualizado el registro de los miembros del CSIRT.
d. Validar que los incidentes estén bien clasificados o en su defecto clasificarlos correctamente.
e. Definir el personal que estará conformando el CSIRT cuando ocurra un incidente.
f. Coordinar el desarrollo de la gestión del incidente.
g. Coordinar con los responsables para la documentación de las acciones realizadas y hechos importantes del incidente, posterior a su resolución.
h. Promover la capacitación del CSIRT para la detección y atención de los incidentes.

E.7.19 Los conocimientos adquiridos a partir de incidentes de seguridad de la información se deben utilizar para reforzar y mejorar los controles de seguridad de la

información. Para ello, posterior a recuperarse del incidente, el CISO junto con el personal que fue involucrado en la atención del incidente, realizará un análisis de lo acontecido, identificarán aspectos de mejora y formularán un plan de acción para realizar las mejoras aplicables.

E.7.20 La UTI debe establecer e implementar procedimientos para la identificación, recopilación, adquisición y preservación de evidencia digital relacionada con incidentes técnicos de seguridad de la información.

E.7.21 Durante una interrupción provocada por un incidente técnico, la UTI debe implementar medidas de seguridad alternativas para mantener la información protegida en tanto se logra la recuperación de los servicios comprometidos. Esto implica evaluar y gestionar los riesgos específicos asociados a la interrupción, así como establecer procedimientos para la comunicación, el respaldo de datos, la recuperación de sistemas críticos y la capacitación del personal en medidas de seguridad durante la interrupción.

E.8 Continuidad del negocio

E.8.1 La CGR deberá desarrollar un Plan de Continuidad del Negocio (BCP) a nivel Institucional. La elaboración e implementación de este plan será coordinada por la UGC, en colaboración con las diferentes áreas de la CGR.

E.8.2 El BCP tiene como objetivo garantizar la continuidad de las funciones y servicios esenciales de la CGR frente a eventos disruptivos. Su finalidad es minimizar las pérdidas y asegurar la reanudación de las operaciones a niveles aceptables dentro de un plazo definido, permitiendo a la CGR seguir cumpliendo con sus funciones y entregando sus productos o servicios de manera oportuna y eficiente.

E.8.3 Como parte de este BCP, la CGR deberá establecer una Comisión de Continuidad del Servicio (CCS) la cual será un equipo de personas con representación institucional destinado a la gestión del BCP. Así mismo, establecerá una Comisión de crisis de continuidad del servicio, con responsabilidades claras para gestionar eventuales crisis (incidentes, desastres o emergencias) a nivel institucional y en coordinación con el CCS.

E.8.4 Será responsabilidad del CCS el definir y dar mantenimiento al BCP, entre otras responsabilidades que se establezcan.

E.8.5 El BCP estará a cargo de un encargado de continuidad quién será el responsable de la gestión e implementación del plan, y otros que lo complementen.

E.8.6 Como parte integral del BCP, la UTI deberá desarrollar y dar mantenimiento a un Plan de Recuperación de Desastres (DRP) de las operaciones de TI alineado al BCP, con el propósito de minimizar el tiempo en que los servicios estarán fuera de operación ante una catástrofe.

E.8.7 La UTI, en coordinación con el encargado de continuidad del negocio, deberá realizar al menos una prueba anual de simulación del funcionamiento del DRP y de la infraestructura de contingencia. Se deberá definir un alcance para las pruebas, particularmente para garantizar que la recuperación de datos sea funcional y que los datos recuperados sean correctos. Estos resultados deben quedar debidamente documentados.

E.8.8 El DRP será activado por la Comisión de crisis de continuidad del servicio, en el momento de presentarse un incidente catalogado como catástrofe, debido a que ha inhabilitado los servicios críticos institucionales y puede haber causado daños en activos tecnológicos, por ejemplo en la infraestructura del centro de cómputo.

E.8.9 La CGR debe definir para los servicios identificados como críticos o esenciales, como parte del DRP y mediante un proceso de Análisis de Impacto del Negocio (BIA) los siguientes tiempos:

- **MTPoD:** Tiempo máximo aceptable que un proceso puede tolerar estar caìdo antes de que haya un impacto. En la CGR se utiliza como el tiempo requerido por los líderes del servicio crítico.
- **RTO:** Tiempo a partir de la caída en donde el producto o servicio debe ser reanudado. Es normalmente definido por la UTI y el CISO.
- **RPO:** Tiempo máximo tolerado de pérdida de información. (la cantidad de datos tolerable que la CGR va a perder sin que genere afectación). Determina el tiempo de pérdida máxima de datos introducidos desde el último backup, hasta la caída del sistema, y no depende del tiempo de recuperación.

E.8.10 La CGR a través de la UTI definirá la estrategia de recuperación que considere adecuada, contemplando en ella una opción para sitio de recuperación en modo contingente al centro de cómputo principal, para garantizar que en caso de un e incidente catalogado como catástrofe, se puedan restablecer los servicios utilizando la información contenida en los respaldos.

E.8.11 El tiempo de reanudación de esta infraestructura contingente para iniciar la carga de la información de respaldos no deberá ser mayor al menor de los tiempos MTPoD definidos para los servicios institucionales que sean soportados por la infraestructura tecnológica.

E.9 Procedimientos de seguridad

E.9.1 La UTI debe documentar todos los procedimientos operativos relacionados con tecnologías de información y ponerlos a disposición del personal que los requiera. Estos procedimientos deben estar actualizados y disponibles para consulta en la intranet institucional, con acceso exclusivo para el personal de la UTI.

E.9.2 El CISO será responsable de supervisar y evaluar periódicamente el cumplimiento de las directrices de seguridad de la información, lineamientos y procedimientos. Se realizarán auditorías regulares para verificar el cumplimiento de las políticas de seguridad de la información. Además, el CISO podrá solicitar a la DGA la realización de estudios de auditoría externa para validar la seguridad de la información institucional.

E.10 Segregación de funciones

E.10.1 La UTI debe implementar controles que garanticen la separación efectiva de tareas críticas y áreas de responsabilidad, especialmente en aquellas funciones que involucran un alto riesgo para la seguridad de la información. Además, se deben establecer esquemas de trabajo con el propósito de mitigar el riesgo de elusión de los controles, conflictos de interés o dejar sin soporte en ausencia del encargado.

E.10.2 La UTI debe implementar medidas para evitar que un solo desarrollador tenga control total sobre un sistema crítico, ya sea en tareas de mantenimiento o de soporte, con el propósito de reducir el riesgo de un único punto de falla y dejar al sistema sin soporte, en caso de la ausencia del encargado.

E.11 Activos Tecnológicos

E.11.1 Todos los activos tecnológicos de la CGR son bienes públicos destinados exclusivamente a satisfacer el cometido público que corresponde a la Institución y no deben ser utilizados para actividades personales.

E.11.2 Cada activo tecnológico tiene asignado un responsable, quien es el encargado de velar por la buena utilización y custodia del recurso de acuerdo con el Reglamento para la administración de los activos y de los bienes en desuso de la Contraloría General de la República.

E.11.3 La computadora debe ser utilizada exclusivamente por el funcionario al que ha sido asignada y no debe ser utilizada por terceras personas. Las labores encomendadas deberán realizarse utilizando la computadora institucional, la cual cuenta con las medidas de seguridad necesarias; y solo en casos debidamente

justificados y autorizados por la UTI, el funcionario podrá utilizar un equipo de su propiedad para realizar sus labores, para lo cual la UTI es responsable de verificar que cuenta con todas las medidas y software de ciberseguridad requeridos. El funcionario deberá aceptar las condiciones que establezca la UTI para la autorización del uso de un computador personal en labores institucionales.

E.11.4 Es responsabilidad del personal de la CGR utilizar los tomacorrientes soportados por la UPS institucional para conectar sus activos tecnológicos. Esto garantiza un nivel adecuado de protección y continuidad en el caso de interrupciones en el suministro eléctrico.

E.11.5 En caso de robo o pérdida del equipo, el funcionario a cargo es responsable de proceder según lo establecido en el Reglamento para la administración de los activos y de los bienes en desuso de la Contraloría General de la República. De igual manera, la jefatura correspondiente deberá informar al CISO en un plazo máximo de un día hábil, para que proceda en coordinación con la UTI, a realizar las acciones necesarias para garantizar la confidencialidad de la información que el equipo pudiera contener localmente o en la nube.

E.11.6 Todo activo tecnológico que almacene información institucional (computadoras, discos duros externos, cintas, usb, grabadoras, etc.) y que deja de ser utilizado, se deberá someter a un proceso de borrado de esta información al momento de dejar de usarla. Para la información de acceso restringido deberá aplicarse un mecanismo de borrado seguro, para lo cual el funcionario gestor de la información deberá informar tal condición al personal técnico que realizará el borrado. Dicha información contempla archivos, cuentas de usuario, correos, y en general cualquier información que no debe ser divulgada. La acción indicada en este apartado deberá ejecutarse al momento de que se le dé criterio técnico por parte de la UTI al equipo previo a su devolución al Almacén.

E.11.7 La gestión de los contratos de mantenimiento de los activos tecnológicos institucionales es competencia de la UTI y la USG.

E.11.8 La CGR proporcionará dispositivos móviles institucionales para el personal que lo requiera en el desempeño de sus funciones, asegurando que estos dispositivos estén configurados con las medidas de seguridad adecuadas.

E.11.9 En caso de pérdida o robo de un dispositivo móvil (personal o institucional) que contenga información institucional, el funcionario deberá reportarlo inmediatamente al CISO y a la UTI para activar los protocolos de seguridad, incluyendo la deshabilitación de acceso y el borrado remoto de datos si es aplicable.

F. Controles de personas

F.1 Vinculación del personal

F.1.1 El proceso de dotación a cargo de la UGPH deberá considerar los presentes lineamientos, con el propósito de que el personal de nuevo ingreso no atente contra los principios y valores institucionales que puedan eventualmente poner en riesgo la seguridad de la información.

F.1.2 La UGPH deberá proporcionar por las vías que se consideren necesarias, al personal de nuevo ingreso, las directrices y lineamientos de seguridad de la información institucionales indicando la obligatoriedad de su acatamiento.

F.1.3 La UGPH reportará oportunamente a la UTI, todos los movimientos de personal, con el fin de que ésta mantenga un registro actualizado de los usuarios de los activos tecnológicos, mediante la creación o eliminación de estos usuarios y sus privilegios básicos dentro del directorio de usuarios o en el medio que la UTI disponga.

F.2 Deberes en la seguridad de la información

F.2.1 Cuando el jerarca o un titular subordinado tenga indicios de que un miembro del personal ha puesto en riesgo la seguridad de la información institucional por uso no apropiado de la misma, deberá comunicarlo al CISO de inmediato. El CISO, en coordinación con la UGPH determinará el procedimiento de investigación y las acciones correspondientes.

F.2.2 Es responsabilidad del personal reportar eventos de seguridad de la información observados o sospechosos a través del correo seguridad.informacion@cgr.go.cr o el Sistema de Órdenes de Servicio (SOS).

F.2.3 El personal es responsable de presentarse en un plazo máximo de 3 días en caso de ser requerido por la UTI para realizar actualizaciones críticas, instalación de software o cualquier situación que lo requiera y no pueda realizarse de forma remota y sea necesaria para garantizar la seguridad de la información.

F.2.4 El CISO deberá realizar validaciones semestrales del cumplimiento que se dé por parte del personal a los lineamientos de seguridad de la información institucional, y comunicará a las jefaturas correspondientes todas aquellas irregularidades detectadas.

F.3 Conciencia de seguridad de la información, educación y capacitación

F.3.1 El CISO realizará campañas de sensibilización para todo el personal en materia de seguridad de la información, para generar conciencia y mantener al personal actualizado sobre amenazas, vulnerabilidades, buenas prácticas y cumplimiento de la normativa institucional.

F.3.2 El CISO desarrollará e implementará programas de capacitación obligatorios para todo el personal, con el objetivo de promover mecanismos de concienciación permanentes y generar una buena cultura digital en seguridad de la información.

F.3.3 El CISO, en coordinación con la UGPH, participará activamente en el proceso de inducción al nuevo personal, dando a conocer el marco de orientaciones internas sobre seguridad de la información, haciendo conciencia en los participantes de la necesidad de gestionar adecuadamente la información con el propósito de minimizar los riesgos de comprometerla.

F.3.4 El CISO realizará procesos regulares de monitoreo del nivel de madurez del personal respecto a la seguridad de la información, detectando los temas sobre los cuales se deben enfocar los esfuerzos de sensibilización.

F.3.5 El CISO con base en los procesos de monitoreo, gestionará campañas de sensibilización en temas de seguridad para todo el personal enfocada en las necesidades detectadas, todo de conformidad con las directrices de comunicación de la CGR vigentes. El CISO deberá validar la efectividad de estas campañas y hacer los ajustes respectivos en caso que lo amerite.

F.3.6 Con el fin de evaluar el nivel de madurez respecto al tema de seguridad de la información, el CISO podrá realizar pruebas de ingeniería social de forma controlada al personal de la Institución.

F.3.7 Con base en los resultados obtenidos de las pruebas de ingeniería social, el CISO, en coordinación con la UGPH, diseñará e implementará programas de capacitación específicos para mejorar el nivel de seguridad relacionados a este tema.

F.3.8 El Despacho Contralor en coordinación con la gerencia de la DGA, la UTI y el CISO, deberá definir y ejecutar un plan de capacitación, formación y actualización para el personal encargado de ejecutar las acciones de seguridad de la información y ciberseguridad, en orden a desarrollar a dicho personal con respecto a un perfil requerido.

F.4 Desvinculación o cambio de labores del personal de la CGR

F.4.1 Es responsabilidad de la UGPH informar oportunamente a la UTI sobre el personal que deje de laborar para la institución, para que el propio día del cese de funciones, proceda con la eliminación de los perfiles y privilegios sobre el uso de los activos tecnológicos asignados.

F.4.2 Cuando se presente un cambio de funciones del personal dentro de una misma dependencia administrativa, el titular subordinado correspondiente deberá informar a la UTI de tal situación, para que se proceda con la eliminación de los privilegios que no le corresponda mantener.

F.4.3 La UTI establecerá los mecanismos mediante los cuales se procederá en estos casos a realizar la eliminación de los perfiles y la baja de los roles y privilegios, registrando el evento en sus bitácoras de control.

F.4.4 Cuando una persona se desvincule de la institución, se aplicarán los siguientes lineamientos, según sea el caso:

F.4.3.1 Si es por renuncia o jubilación y previo al cese de sus funciones, la persona deberá extraer del equipo a él asignado, la información personal y trasladar al titular subordinado correspondiente la información laboral. De igual manera deberá trasladar aquella información que tenga en su espacio de almacenamiento en la nube.

F.4.3.2 Si es por despido, la UGPH coordinará con la UTI y la persona cesada o con algún representante previamente definido y comunicado a la jefatura, la extracción de la información personal que tuviera almacenada. Igualmente coordinará con el titular respectivo, para la extracción y traslado de la información laboral que tenga esa persona, incluyendo lo que tenga almacenado en el espacio asignado de almacenamiento en la nube.

F.4.3.3 Si es por fallecimiento, la UGPH coordinará con la UTI y con los familiares de la persona fallecida o con algún representante previamente definido y comunicado a la jefatura, la extracción de la información personal que tuviera almacenada en la carpeta establecida para estos propósitos. Igualmente coordinará con el titular respectivo, para la extracción y traslado de la información laboral que tenga esa persona, incluyendo lo que tenga almacenado en el espacio asignado de almacenamiento en la nube.

F.4.3.4 En cualquiera de los casos anteriores, una vez que se ha extraído la información del equipo, el responsable de su custodia deberá devolver el equipo al almacén,

con el previo criterio técnico emitido por la UTI, que contempla la ejecución del borrado del perfil de usuario y la información almacenada en el disco duro, para la reasignación o disposición del activo.

F.4.3.5 Cuando una persona se suspende en sus funciones, o se le otorgan permisos con o sin goce de salario, la jefatura respectiva o la UGPH deberá definir los privilegios que se le mantienen o revocan y gestionar con la UTI la aplicación de la medida.

F.4.3.6 Previo al cese de sus funciones, la persona deberá trasladar al titular subordinado correspondiente o a quien éste defina, la información laboral contenida en su espacio de almacenamiento asignado en la nube. En los casos en que una persona deja de laborar para la institución, el titular subordinado correspondiente podrá coordinar con la UTI si desea que la información que esa persona haya dejado en la nube sea trasladada a esa jefatura o a otro funcionario quien ésta defina. En todo caso, el día de rige del cese de funciones, de mantenerse todavía información en el espacio de almacenamiento en la nube asignado a la persona, la UTI procederá a trasladar a la jefatura de la persona que cesa funciones o a la persona quien ésta haya definido, y ese mismo día procederá a eliminar la cuenta de correo electrónico con toda la información de correos contenida, eliminando igualmente el espacio de almacenamiento en la nube asociado a esa cuenta.

F.4.3.7 El personal que cese sus labores en la CGR debe respetar los acuerdos de confidencialidad suscritos, así como las condiciones de confidencialidad establecidas en la normativa interna.

F.4.3.8 Al momento en que una persona deje de laborar para la Institución, o se encuentre con permiso sin goce de salario, la UGPH informará a la USG para que proceda a suspender cualquier acceso asignado para ingresar a las instalaciones. Los dispositivos de acceso asignados a esta persona deberán ser devueltos a la UGPH al momento en que deje de laborar para la institución.

F.5 Teletrabajo

F.5.1 El personal es responsable de mantener sus equipos actualizados, incluyendo la instalación y actualización del antivirus, así como la aplicación de parches y actualizaciones del sistema operativo. La UTI proporcionará las herramientas y el soporte necesario para facilitar estas tareas, y realizará monitoreos periódicos para verificar el cumplimiento de esta responsabilidad.

F.5.2 El personal debe asegurarse de contar con una fuente de energía eléctrica confiable, con al menos una regleta para protección y preferiblemente utilizar una

UPS para proteger sus equipos y garantizar la continuidad del servicio.

F.5.3 Con respecto a la seguridad de la red, utilizar contraseñas robustas para la red inalámbrica de su hogar. Si se va a conectar en otra ubicación distinta a su hogar, debe activar el VPN.

F.5.4 El personal es responsable de mantener un escritorio y pantalla limpios, de acuerdo con la sección “Escritorio y pantalla limpios“ de este documento.

F.5.5 El personal es responsable de asegurar la protección física y lógica de los activos institucionales cuando se encuentren fuera de las instalaciones de la CGR. Para ello, debe transportar los equipos en estuches o maletines adecuados que ofrezcan protección contra golpes y caídas, y no dejarlos sin supervisión en lugares públicos o vehículos. Además, al trabajar en ubicaciones externas, debe asegurarse de que el entorno es seguro y no existen riesgos visibles de robos o acceso no autorizado.

G. Controles físicos

G.1 Perímetro de seguridad física

G.1.1 Todo acceso a las instalaciones por parte del personal debe ser registrado por medio del SIRET[4] debe realizarse utilizando el carné de identificación institucional.

G.1.2 El acceso a los espacios de coworking de la CGR por parte del personal debe ser controlado mediante un sistema de control de acceso.

G.1.3 Los accesos comunes del personal y visitantes se realizarán con las siguientes consideraciones:[5]

G.1.2.1 Los visitantes que acceden a la Institución, deben ser autorizados por algún miembro del personal como responsable del ingreso. Se debe registrar su ingreso y portar durante su estadía en las instalaciones en un lugar visible, un distintivo de identificación que indique el piso a visitar. En los casos en donde sea una visita general, la autorización será realizada por el oficial de seguridad.

G.1.2.2 Los ingresos vehiculares al parqueo interno del edificio principal tanto del personal como visitantes se deben realizar con las siguientes consideraciones:

G.1.2.3 Si es ingreso vehicular del personal:

[4] Sistema Institucional de Registro de Espacios de Trabajo
[5] Accesos comunes se refiere a accesos de personas a pie.

- Personal con ingreso específico para recoger o dejar algún material de trabajo: Debe pedir la autorización al oficial de seguridad y presentar el carné de identificación.

G.1.2.4 Para el ingreso vehicular de visitantes:

- La USG debe definir un protocolo para el ingreso de visitantes, proveedores y visitantes especiales de carácter oficial, el cual debe incluir la identificación de los ocupantes del vehículo, motivo de la visita y tiempo estimado de permanencia.

G.1.2.5 En eventos de capacitación la autorización de ingreso estará soportada por una lista con los nombres de los participantes, misma que deberá ser remitida oportunamente a la USG por parte del organizador del evento.

G.1.2.6 Es responsabilidad de los oficiales de seguridad solicitar a los visitantes en el momento que se retiran de las instalaciones de la CGR, el distintivo de identificación entregado. En caso de no portarlo se aplicará el protocolo correspondiente.

G.1.2.7 Cuando un visitante se retira de las instalaciones según lo indicado en el punto anterior, se debe registrar su salida en el sistema (ya sea que la registre el oficial o se haga de forma automática). Esto con el propósito de contar con información de las personas que permanecen en las instalaciones.

G.1.2.8 La USG se encargará de elaborar las guías correspondientes para aplicar en el control habitual de ingreso del personal y visitantes así como en los casos particulares relacionados.[6]

G.1.2.9 Si algún miembro del personal detecta a un visitante en un piso diferente al indicado en el gafete de identificación, deberá reportarlo de inmediato a los oficiales de seguridad.

G.1.2.10 Las instalaciones deben ser monitoreadas continuamente para detectar y disuadir accesos físicos no autorizados.

G.2 Protección contra amenazas físicas y ambientales

G.2.1 La UTI, en coordinación con la USG, implementará medidas de seguridad ambiental en el centro de cómputo para proteger la infraestructura tecnológica. Estas medidas incluirán sistemas de detección y extinción de incendios, control de

[6] Por ejemplo los casos en donde el personal no porte carné, cuando un visitante se encuentre en sitios distintos a los autorizados, un visitante se retire sin portar el carné o en los casos de visitantes especiales que ingresan en vehículo sin que se les entregue el carné

temperatura y humedad, y protección eléctrica con sistemas de alimentación ininterrumpida (UPS) y generadores de energía de respaldo.

G.2.2 La USG es la responsable del monitoreo de la correcta operación de los equipos de seguridad ambiental en funcionamiento dentro del centro de cómputo. La USG deberá definir las guías correspondientes de monitoreo con el fin de evaluar el funcionamiento de estos equipos, aplicar medidas correctivas y minimizar de esta forma la posibilidad de algún evento que ponga en riesgo los equipos y consecuentemente la información residente en los servidores institucionales.

G.2.3 En cuanto a otros recintos donde existan activos de información[7], sin importar el medio en que la información se encuentre, la USG deberá proveer los mecanismos de protección necesarios contra amenazas ambientales.

G.2.4 La UTI desarrollará planes de acción para proteger la plataforma tecnológica ante la eventualidad de fenómenos naturales, incluyendo procedimientos para la protección de equipos y sistemas ante la caída de ceniza, arena, polvo u otros elementos dañinos, así como planes de contingencia para enfrentar eventos climáticos extremos como huracanes, terremotos, incendios e inundaciones. Estos planes de acción deberán estar integrados en el Plan de Continuidad del Negocio (BCP) de la CGR.

G.3 Protección del centro de cómputo y cuartos de comunicación

G.3.1 Todos los servidores de la CGR deben estar ubicados en zonas de acceso físico restringido con algún mecanismo de control de acceso y grabación de video.

G.3.2 El acceso al centro de cómputo estará restringido al personal autorizado. Cualquier persona no autorizada que requiera ingresar deberá registrarse en una bitácora, indicando su nombre, identificación, motivo del ingreso y hora de entrada y salida. El ingreso deberá ser autorizado y supervisado en todo momento por un representante de la UTI, quien será responsable de la seguridad del área durante la visita.

G.3.3 Todos los cuartos de comunicaciones deben contar con control de acceso físico que contemple al menos control de apertura de puertas.

G.3.4 No se permite ingresar con alimentos o bebidas a los cuartos donde se encuentren los servidores institucionales, ni a los cuartos de comunicaciones en cada piso.

[7] Por ejemplo los cuartos de comunicación ubicados en los distintos pisos de los edificios de la CGR

G.3.5 No se permite ingresar o utilizar elementos que almacenen o transporten líquidos o materiales corrosivos o inflamables a los recintos donde se encuentren servidores institucionales o en los cuartos de comunicaciones, a excepción de aquellos requeridos para la operación del sistema de protección contra incendios.

G.3.6 El personal de limpieza que trabaje en el centro de cómputo recibirá capacitación específica por parte de la UTI, en coordinación con la USG, sobre los cuidados y precauciones necesarios para evitar dañar los equipos y la infraestructura tecnológica.

G.3.7 El centro de cómputo debe estar protegido contra los cortes de energía y otras interrupciones causadas por fallos en los servicios públicos para evitar la pérdida o daño de la información y la interrupción de las operaciones.

G.3.8 Los cables de energía, datos y comunicaciones deben estar protegidos mediante canaletas, ductos o bandejas para prevenir daños físicos, interferencias y accesos no autorizados. Se utilizarán materiales y técnicas de instalación que minimicen el riesgo de interceptación o manipulación de la información.

G.3.9 El equipo del centro de cómputo se debe mantener correctamente para asegurar la disponibilidad, integridad y confidencialidad de la información. Para ello se debe:

- **a.** Realizar un mantenimiento regular y preventivo del equipo de cómputo incluyendo limpieza física, actualización de software y firmware.
- **b.** Mantener un ambiente controlado en términos de temperatura y humedad.

G.3.10 Los componentes de los equipos de infraestructura que contengan medios de almacenamiento, se deben verificar para asegurarse de que los datos sensibles y el software con licencia se han eliminado o sobrescrito de forma segura antes de su desecho o reutilización.

G.4 Áreas donde se encuentren documentos físicos con información de acceso restringido

G.4.1 Los espacios donde se manejen documentos físicos con información de acceso restringido, deben contar con un control de acceso físico solo para el ingreso de personas autorizadas.

G.4.2 En el caso específico del archivo central, debe quedar un registro documental de las personas que ingresan a esta área.

G.4.3 La USI deberá definir los controles correspondientes para el manejo de documentos físicos que contengan información de acceso restringido.

G.5 Escritorio y pantalla limpios

G.5.1 El personal es responsable de apagar o bloquear la pantalla al momento de ausentarse de su escritorio y no dejar expuestos medios de almacenamiento que contengan información de acceso restringido (USB, CD, discos duros externos, etc), para evitar cualquier uso no autorizado de su equipo.

G.5.2 El personal deberá velar por mantener la seguridad de la información de acceso restringido contenida en documentos físicos que se utilicen en el cumplimiento de las funciones asignadas, considerando al menos:

- Si se tienen documentos en el escritorio, no dejarlos expuestos a la vista de terceras personas. Al contener información de acceso restringido estos documentos deberán mantenerse resguardados bajo llave y con acceso sólo a personal autorizado.
- Los documentos que contengan información de acceso restringido deben tener una identificación visible que los diferencie del resto de documentos.
- No tener contraseñas escritas en lugares visibles.

G.5.3 Cuando se impriman documentos que contengan información de acceso restringido, se debe velar por no dejar documentos desatendidos en la impresora o en la cola de impresión.

G.5.4 Los documentos impresos que contengan información de acceso restringido deben destruirse de forma segura antes de ser desechados, utilizando una trituradora de papel o un proceso de destrucción que garantice que la información no pueda ser recuperada.

G.5.5 Al finalizar una reunión o sesión de trabajo, se deben borrar las pizarras, o cualquier otro elemento utilizado para exponer información, especialmente si se ha tratado información de acceso restringido.

G.5.6 El equipo portátil debe estar asegurado con candado de seguridad cuando su encargado no se encuentre presente en el escritorio.

H. Controles tecnológicos

H.1 Acceso lógico

H.1.1 Todo el personal tendrá asignada una identidad digital intransferible, compuesta por un nombre de usuario y una contraseña, o bien un certificado digital reconocido

por la CGR. Bajo ninguna circunstancia se debe entregar a terceras personas esas credenciales.

H.1.2 El personal es responsable de todas las acciones realizadas con la identidad digital asignada, salvo en los casos en los cuales se demuestre que ese mecanismo de identificación ha sido vulnerado y no responde a una falta de cuidado de su parte.

H.1.3 La autenticación con dos factores (2FA) deberá utilizarse de manera obligatoria en todas las soluciones tecnológicas que lo permitan. La UTI implementará la autenticación con dos factores para los sistemas institucionales, medida que aplicará de manera igualmente obligatoria.

H.1.4 No se permite la creación de cuentas de usuario impersonales, excepto casos debidamente valorados y aprobados por la UTI. Para esto debe haber una solicitud formal de la Unidad correspondiente. Debe quedar registrado por la UTI la persona responsable de dicha cuenta impersonal y la UTI debe llevar un registro documental de las cuentas asignadas bajo esta modalidad.

H.1.5 La UTI debe definir y administrar las guías para la asignación, mantenimiento y revocación de las identidades digitales asignadas al personal.

H.1.6 La UTI debe promover la revisión periódica y la adecuación de los privilegios de acceso a la infraestructura tecnológica, basándose en el principio de menor privilegio, con el objetivo de prevenir privilegios excesivos que puedan comprometer la seguridad.

H.1.7 Las contraseñas deben cumplir con los estándares de robustez definidos por el CISO e implementados por la UTI. Estos estándares se basarán en las mejores prácticas y considerarán la longitud mínima, expiración periódica, la complejidad y la no repetición de contraseñas anteriores.

H.1.8 Todo el personal deberá utilizar un administrador de contraseñas seguro aprobado por la UTI y el CISO para almacenar sus contraseñas. Se prohíbe el almacenamiento de contraseñas en navegadores web u otros medios no seguros.

H.1.9 Cuando se requiera acceder un sistema de información y no se encuentre el responsable de la cuenta, la UTI, previa autorización de la jefatura correspondiente, procederá a extraer la información requerida utilizando los mecanismos que considere necesarios. Este procedimiento debe quedar documentado.

H.1.10 Todos los servidores de la plataforma tecnológica de la CGR deben contar con

firewall habilitado como parte del software instalado dentro del equipo, que garantice acceso seguro al servidor y protección contra intrusos.

H.1.11 La información propia de la configuración de cada firewall institucional se considera de acceso restringido y debe manejarse siguiendo las recomendaciones establecidas respecto al manejo de este tipo de información.

H.1.12 Los componentes del sistema de firewall institucional deben ubicarse en zonas de acceso físico restringido.

H.1.13 La UTI cuando proceda, debe eliminar o cambiar la contraseña de todas las cuentas de usuario pre-instaladas en los activos TIC que se adquieren. Estas contraseñas deben cumplir con las medidas de seguridad definidas por el CISO.

H.1.14 Los usuarios patrocinadores de los sistemas de información de la CGR definirán los roles y privilegios de acceso que aplicarán a los perfiles de usuarios de las aplicaciones. Mediante estos roles se establecerá la segregación de funciones y la delegación de acciones. La UTI implementará estos roles y privilegios conforme a los requerimientos de los patrocinadores.

H.1.15 Las jefaturas son responsables de gestionar los roles y privilegios de acceso de los usuarios a su cargo, solicitando a los administradores de activos TIC o de sistemas la asignación o revocación de permisos según las necesidades y responsabilidades de cada usuario.

H.1.16 La UTI pondrá a disposición de las jefaturas por los medios que se consideren oportunos, información de los roles y privilegios asignados al personal bajo su cargo. Es responsabilidad de la jefatura correspondiente o quien ésta haya asignado, verificar que estos roles y privilegios estén alineados a las funciones realizadas por su personal y solicitar a los responsables de administrar los activos TIC, los ajustes necesarios para garantizar la seguridad de la información.

H.1.17 El acceso a los sistemas y datos en producción por parte de los usuarios, se realizará únicamente mediante los aplicativos existentes. Los desarrolladores de sistemas no deben tener acceso a modificar los sistemas y datos en producción. En los casos en los cuales no existe un aplicativo que permita la modificación de la información, ésta se podrá hacer previa coordinación entre el administrador del sistema y la UTI y deberá quedar debidamente documentado.

H.1.18 En el caso particular de que se requiera acceso a los datos en producción[8], sea de

[8] Se refiere específicamente a datos contenidos en las Bases de Datos utilizadas por los sistemas en producción, ya sean de la CGR o de otras Instituciones, En el caso de ser de otras Instituciones

bases de datos internas de la CGR o de otras Instituciones, para uso en plataformas de ETL; estos datos deberán ser accedidos únicamente por personal de la UTI designado formalmente por la jefatura de esta unidad, utilizando las herramientas disponibles para la extracción de los datos y acatando las recomendaciones emitidas en la guía específica de seguridad para ambientes de almacenes de datos.

H.1.19 Los sistemas de información deben contar con la facilidad de generar registros en archivos de bitácoras para permitir una trazabilidad de las acciones realizadas sobre las bases de datos. El CISO junto al responsable funcional del sistema, definirán la información que será registrada en estas bitácoras.

H.1.20 Las contraseñas de los servidores institucionales y de cualquier otro equipo que lo requiera, deben ser registradas y custodiadas por el jefe de la UTI utilizando algún mecanismo seguro y encriptado, al cual tendrá acceso en caso de ser necesario el coordinador del área de infraestructura de la UTI o las personas que el jefe de la UTI designe.

H.1.21 La UTI periódicamente deberá realizar, procesos de reforzamiento[9] para mitigar vulnerabilidades técnicas de los servidores institucionales.

H.1.22 La UTI debe llevar un registro documental de todos los servidores institucionales que estén publicados o visibles desde la internet, indicando los servicios habilitados en cada uno.

H.1.23 Por ninguna circunstancia un usuario debe, sin autorización expresa de la UTI, utilizar el computador asignado como servidor de servicios no autorizados, como por ejemplo FTP, Telnet, web, carpetas compartidas o servidor de chat.

H.1.24 La UTI implementará las medidas necesarias para proveer en el servicio DNS las condiciones de seguridad que el CISO defina.

H.1.25 El responsable de la administración de los DNS debe ejecutar cada seis meses procedimientos para validar la funcionalidad de estos servicios y documentar este proceso.

H.1.26 La UTI es la unidad responsable de la coordinación con el proveedor de servicios

podrían ser Bases de Datos colocadas por la Institución en un sitio para el acceso por parte de la CGR

[9] Del inglés Hardening. Consiste en una serie de acciones sobre los servidores que pretenden la reducción de vulnerabilidades en los mismos, eliminando software, servicios, usuarios, innecesarios en el sistema; cerrando puertos que no estén en uso, asignando password robustos y aplicando actualizaciones publicadas por los proveedores

de Internet (ISP) y con la autoridad latinoamericana de asignación de direcciones (LACNIC), para la gestión de direcciones IP públicas.

H.1.27 La UTI es la responsable de coordinar con la autoridad administradora de dominios a nivel nacional, para cualquier aspecto relacionado con los dominios de la CGR.

H.1.28 El personal que opte por utilizar dispositivos móviles personales (smartphones y tablets) para realizar funciones laborales que involucren información institucional, deberán registrarlos ante la UTI y aceptar las políticas de seguridad establecidas. La UTI, en coordinación con el CISO, verificará el cumplimiento de las políticas de seguridad y ciberseguridad requeridas para estos dispositivos.

H.1.29 Se deberá implementar una solución de gestión de dispositivos móviles, que asegure que la información institucional en dispositivos personales esté protegida por contraseña o biometría, cifrado de datos y que permita la segregación de datos corporativos y personales, y la eliminación remota selectiva de datos institucionales en caso de pérdida, robo o desvinculación del personal.

H.2 Comunicaciones electrónicas

H.2.1 El chat institucional debe utilizarse para comunicaciones internas breves y concisas relacionadas con el trabajo. Se debe evitar el uso del chat para conversaciones personales.

H.2.2 Se prohíbe el uso de aplicaciones de mensajería externas, como WhatsApp, para el intercambio de información confidencial o de acceso restringido, con el fin de garantizar la seguridad de la información y el cumplimiento de las políticas institucionales.

H.2.3 El servicio de correo electrónico institucional es el medio oficial de comunicación electrónica de la CGR y está destinado a satisfacer el cometido público que corresponde a la Institución así como las necesidades de comunicación del personal.

H.2.4 A solicitud de la UGPH, la UTI asignará una cuenta de correo electrónico al personal de la CGR así como a las organizaciones y agrupaciones debidamente autorizadas por aquella Unidad. Tratándose del personal, la cuenta se mantendrá activa en tanto se encuentren laborando en la Institución o tengan un permiso con o sin goce de salario. Una vez que se pierda esta condición de personal de la CGR, la UGPH informará a la UTI la situación y ésta procederá a eliminar la cuenta. Con la eliminación de la cuenta se borran todos los correos que al momento tenga almacenados sin posibilidad de recuperarlos, así como las

comunicaciones del chat y los archivos que tenga almacenados en su espacio de nube.

H.2.5 La información contenida en los buzones de correo electrónico de cada persona, es privada y pertenece al usuario titular de la cuenta. Toda comunicación emitida o recibida por una persona desde la cuenta de correo electrónico es de su responsabilidad y debe velar por no comprometer la imagen ni la credibilidad de la CGR con las comunicaciones que realice.

H.2.6 Todo correo electrónico que transfiera información de acceso restringido ya sea como parte del mensaje o como archivo anexo al mismo deberá considerar los lineamientos que le apliquen, indicados en este documento. En este sentido, la UTI dispondrá de tecnología apropiada para que en estos casos los mensajes cuenten con autenticidad, integridad y seguridad.

H.2.7 Se entenderá como correo masivo el enviado de forma general o impersonal a un grupo de cuentas. En tales casos, los destinatarios de los correos y/o el nombre del grupo al que se envían, se deben incluir en el campo CCO (Copia oculta) del mensaje de correo, esto con el fin de no dar respuestas masivas a estos correos electrónicos y como medida de protección de la privacidad de las direcciones de correo.

H.2.8 El envío de correos al grupo masivo denominado “Funcionarios CGR” está permitido únicamente para aquellos usuarios que hayan sido autorizados por la UTI y las instancias responsables.

H.2.9 Los grupos de representación internos de la CGR podrán crear un espacio dentro del área de suscripción de la intranet institucional. Para esto deberán realizar la solicitud al grupo de coordinación estratégica del proceso de comunicación interna y acatar lo indicado en la Directrices de Comunicación Interna de la CGR. La UTI será la responsable de crear los grupos y el comité de coordinación estratégica es el responsable de publicar dentro del sitio de la intranet institucional los vínculos a las secciones propias de cada uno de estos grupos. Las publicaciones realizadas en cada uno de estos espacios asignados para los grupos de representación internos de la CGR se le enviarán por correo a cada uno de los miembros del personal que se hayan suscrito de manera voluntaria a dichos grupos.

H.2.10 La UTI tendrá la potestad de bloquear a nivel institucional, la recepción de correos electrónicos de un remitente o un dominio externo, cuando se determine que son correos no deseados o spam y están siendo enviados a una gran cantidad de personas.

H.2.11 La UTI podrá crear cuentas de correo impersonales dependiendo de la conveniencia institucional, previa valoración del caso y con la autorización del Gerente de División de la Unidad solicitante. Para la atención de estos casos el interesado deberá plantear una solicitud formal ante la UTI para que sea valorada. Deberá quedar registrado por la UTI la persona o personas responsables del uso de dicha cuenta impersonal y será responsabilidad de la jefatura correspondiente informar a la UTI cualquier cambio en estos responsables, para que la UTI proceda a asignar o eliminar los privilegios asociados.

H.3 Controles de software

H.3.1 Todos los programas instalados en la plataforma tecnológica deben ser autorizados previamente por la UTI, para verificar su seguridad y legalidad. Esto aplica para software con licencia, de código abierto o de software libre. Además la UTI es responsable de mantener un inventario actualizado de los mismos.

H.3.2 En el caso de que una persona requiera instalar un nuevo programa o acceder a un sitio web no autorizado institucionalmente, deberá solicitar la autorización correspondiente a su superior jerárquico. Este último presentará la solicitud de autorización ante la UTI, quien, en coordinación con el CISO, realizará un análisis técnico y de seguridad para, de ser el caso, autorizar el uso del programa o el acceso al sitio web solicitado.

H.3.3 El personal no podrá copiar ni traspasar a terceros licencias de software o desarrollos realizados por y para la CGR, a no ser que exista de previo un convenio interinstitucional que lo respalde.

H.3.4 La UTI se apoyará en procesos automatizados de inventario del software instalado en las estaciones de trabajo para detectar y desinstalar cualquier programa no autorizado. Estos procesos se deben realizar de forma mensual.

H.3.5 La UTI debe implementar controles para bloquear la línea de comandos (CMD) y Powershell en todos los dispositivos, excepto en aquellos casos donde se cuente con la aprobación explícita de la UTI y el CISO. Se mantendrá un registro de los dispositivos con acceso habilitado y las justificaciones para dicha excepción.

H.3.6 El reloj de todos los dispositivos de procesamiento de la información de la CGR se deben sincronizar con servidores de marca de tiempo, utilizando el Protocolo de Tiempo de Red (NTP).

H.4 Protección contra malware

H.4.1 Todas las computadoras y cuando aplique, otros dispositivos, deben contar con un

programa antimalware activo, actualizado y aprobado por la UTI.

H.4.2 La UTI será la responsable de la gestión del antimalware instalado en los distintos equipos institucionales, garantizando que los equipos estén debidamente licenciados, operativos y actualizados.

H.4.3 Es responsabilidad del usuario vigilar que la versión del antimalware instalado en el equipo asignado, se encuentre actualizada y operando satisfactoriamente. En caso contrario deberá informar a la UTI por los medios definidos, para proceder con la debida corrección.

H.4.4 Es responsabilidad del personal informar a la UTI por el canal formalmente establecido, en el momento de detectar algún malware o un comportamiento anormal sobre el equipo en uso.

H.4.5 El CISO es responsable de monitorear permanentemente la existencia interna o externa a la Institución, de programas maliciosos (malware) y coordinar con los encargados de infraestructura, de aplicar las medidas preventivas y correctivas para minimizar el riesgo de contagio por parte de los equipos institucionales.

H.4.6 La UTI deberá coordinar con el proveedor del servicio de correo en la nube para que valide el estado de salud[10] de los correos electrónicos que entren o salgan del dominio de la CGR y elimine o ponga en cuarentena todos aquellos correos detectados con malware.

H.4.7 La UTI es responsable de implementar y gestionar, mediante la utilización de dispositivos y herramientas de seguridad especializadas, un sistema de defensa que permita la detección y bloqueo de ataques o accesos no autorizados a los equipos y redes institucionales.

H.4.8 El personal es responsable de utilizar los equipos asignados de forma segura y responsable, siguiendo las mejores prácticas y directrices de seguridad establecidas y comunicadas por la UTI y el CISO, para minimizar el riesgo de infección por malware. Estas prácticas incluyen:

- Validar orígenes confiables de correos electrónicos (dominios desconocidos o que causen sospecha, mensajes que soliciten datos personales, contenido no coherente con el remitente, correos con links a sitios web desconocidos).

[10] Estado de salud se refiere al hecho de que el mensaje cumpla con las condiciones de seguridad. establecidas por la UTI para garantizar que el correo no comprometa la seguridad de la información.

- Evitar compartir información personal o confidencial en sitios web que no utilicen protocolos de seguridad como HTTPS.
- Antes de conectar cualquier dispositivo externo (discos duros, memorias USB, smartphones, etc.) a los equipos institucionales, escanearlos con la solución antimalware para asegurar que no contengan malware.
- Asegurar que el software de seguridad, incluyendo el antimalware, esté instalado, activo y actualizado.
- Evitar conectar el equipo a redes desconocidas o catalogadas como inseguras.
- No conectar dispositivos de almacenamiento externo encontrados o de origen desconocido a los equipos institucionales. Reportar el hallazgo a la UTI para que verifiquen la seguridad del dispositivo antes de su uso.

H.4.9 Cuando proveedores externos necesiten transferir archivos a servidores institucionales, se debe implementar un proceso de validación de la integridad y seguridad de dichos archivos. Este proceso debe incluir, como mínimo, el escaneo con soluciones antimalware actualizadas y la verificación de la ausencia de código malicioso o contenido inapropiado.

H.4.10 Todo equipo institucional que cuente con un medio de conexión inalámbrico deberá desactivar la conexión *bluetooth* a no ser que sea requerida por alguna aplicación.

H.5 Gestión de vulnerabilidades técnicas

H.5.1 El CISO, en coordinación con la UTI, deberá ejecutar al menos una vez al año un análisis de vulnerabilidades sobre los equipos de la plataforma tecnológica. Los resultados del análisis se documentarán en un informe que incluya recomendaciones para la mitigación de las vulnerabilidades encontradas. El CISO y la UTI definirán un plan de acción para implementar las medidas correctivas necesarias y dar seguimiento a su efectividad.

H.5.2 La UTI debe mantener un registro documental completo y actualizado de todas las vulnerabilidades detectadas en la infraestructura tecnológica de la institución. Este registro debe incluir la descripción de cada vulnerabilidad, su nivel de riesgo, las fechas de detección y mitigación, y el plan de acción implementado para su corrección.

H.5.3 El CISO es el responsable de dar seguimiento a la aplicación de las medidas de remediación implementadas por la UTI respecto a los hallazgos y recomendaciones encontrados en el estudio de vulnerabilidades.

H.6 Gestión configuraciones y cambios

H.6.1 Todas las configuraciones de los equipos de hardware, software, servicios y redes se deben establecer, documentar, implementar, monitorear y revisar.

H.6.2 La UTI deberá desarrollar una metodología para la gestión de cambios a los activos TIC bajo su responsabilidad.

H.6.3 La UTI deberá establecer como parte de esta metodología, las acciones por realizar para cada uno de los siguientes tipos de cambios sobre los activos TIC.

- Cambio normal: Son aquellos requerimientos de cambio con un procedimiento establecido que **requieren aprobación** del responsable de la gestión del cambio.
- Cambio de emergencia o urgente: Son requerimientos de cambio de alta prioridad que por la premura deben seguir un proceso expedito.
- Cambio pre-aprobado o estándar: Son cambios **previamente definidos y aprobados**. Son de bajo riesgo, relativamente frecuentes y siguen un procedimiento conocido por la persona encargada de la gestión del cambio.

H.7 Gestión de datos

H.7.1 La información almacenada en las bases de datos, sistemas de información, dispositivos o en cualquier otro medio de almacenamiento deberá ser eliminada de forma segura cuando ya no sea necesaria para cumplir con los fines para los que fue recolectada, para evitar la exposición innecesaria de información confidencial de acuerdo con las políticas institucionales.

H.7.2 Se implementarán técnicas de enmascaramiento de datos para proteger la información clasificada como sensible, en entornos de desarrollo, pruebas y cualquier otro escenario donde no se requiera el acceso a los datos originales. La UTI, en coordinación con el CISO y los propietarios de la información, definirá los métodos de enmascaramiento apropiados para cada tipo de dato y sistema, asegurando la protección de la información confidencial sin afectar la funcionalidad de las aplicaciones.

H.7.3 Para prevenir la fuga de información sensible, se implementarán medidas de seguridad en todos los sistemas, redes y dispositivos que procesen, almacenen o transmitan dicha información. Estas medidas incluirán, entre otras, el control de acceso, el cifrado de datos, la prevención de pérdida de datos (DLP) y el análisis de tráfico de red. La UTI, en coordinación con el CISO, definirá las medidas específicas a implementar en cada caso, basándose en el tipo de información, el

nivel de riesgo y las tecnologías disponibles.

H.8 Respaldo de información

H.8.1 Respaldo de bases de datos institucionales

H.8.1.1 Toda la información digital catalogada como crítica o de acceso restringido y cualquier otra previamente definida, debe contar con un proceso periódico[11] de respaldos en un sitio externo a las instalaciones del edificio principal de la CGR.

H.8.1.2 La UTI elaborará y mantendrá actualizadas guías claras y concisas para el manejo de los respaldos de información, incluyendo los procedimientos para la creación y la verificación de la integridad de los mismos, el almacenamiento seguro y la recuperación de la información en caso de ser necesario.

H.8.1.3 Todo traslado de información de respaldo que se realice fuera del centro de cómputo, ya sea traslado físico o digital (incluyendo la nube), deberá realizarse siguiendo un procedimiento que garantice la seguridad de la información.

H.8.1.4 La UTI realizará pruebas de restauración de respaldos de información al menos dos veces al año, para verificar la integridad, disponibilidad y recuperabilidad de la información respaldada. Estas pruebas se realizarán en fechas definidas en coordinación con la jefatura de la UTI, y sus resultados se documentarán formalmente, incluyendo cualquier incidente o problema detectado durante el proceso de restauración, así como las acciones correctivas implementadas.

H.8.2 Respaldo de información de estaciones de trabajo

H.8.3.1 El personal de la CGR es responsable del mantenimiento, custodia y respaldo de la información que mantiene en su estación de trabajo.

H.8.3.2 En el disco duro de las estaciones de trabajo asignadas al personal, deben existir dos carpetas designadas claramente para almacenar la información: una para asuntos laborales y otra para asuntos personales.

H.8.3.3 Los respaldos de la información contenida en las estaciones de trabajo, se harán en el espacio asignado en la nube y solo si es necesario, en unidades de almacenamiento auxiliar tales como llaves USB, discos externos en cuyo caso el usuario es el responsable de su custodia.

H.8.3.4 Cuando se realicen respaldos en dispositivos de almacenamiento auxiliar, el responsable de la custodia de estos dispositivos debe velar por la seguridad física

[11] Esta periodicidad será definida por la UTI según criterios definidos en el análisis de impacto del negocio.

de los mismos y borrar la información contenida en ellos cuando no se requiera más.

H.8.3.5 El personal es responsable de realizar un respaldo de su información, previo a cualquier actividad de mantenimiento por parte de la UTI o de terceras personas.

H.8.3 Respaldo de aplicaciones y ambiente de producción

H.8.3.1 La UTI es la responsable de tener un respaldo externo[12] debidamente actualizado del software e imágenes del sistema del ambiente de producción, que sirva de sustento en la recuperación de los sistemas de misión crítica en el menor tiempo posible.

H.9 Control de bitácoras

H.9.1 La UTI debe implementar un sistema centralizado de gestión de eventos de seguridad (SIEM) que recopile y analice los registros de eventos (logs) de todos los servidores, dispositivos de red y equipos de seguridad de la plataforma tecnológica. Este sistema permitirá la monitorización en tiempo real de la actividad en la red, la detección de eventos sospechosos y la generación de alertas para la investigación y respuesta a incidentes de seguridad.

H.9.2 Estos registros deben considerar situaciones como actividades realizadas por los usuarios, así como las excepciones, las fallas y los eventos relacionados con situaciones que puedan poner en riesgo la seguridad de la información. El detalle y tiempo de retención de la información que se grabará en estas bitácoras, se definirá en coordinación del CISO con la UTI.

H.9.3 La UTI deberá implementar las medidas de seguridad necesarias para la protección de estos servidores de logs contra accesos no autorizados.

H.9.4 La UTI validará mensualmente, utilizando los mecanismos que considere necesarios, el correcto funcionamiento de estos servidores de logs.

H.9.5 La UTI debe establecer un procedimiento de monitoreo continuo de la información de los servidores de logs, con el fin de detectar y responder a cualquier anomalía o evento que pueda poner en riesgo la seguridad de la información.

[12] En un sitio fuera de las instalaciones principales de la CGR, para que en caso de una catástrofe que afecte las instalaciones del Centro de Cómputo, el contenido de estos respaldos no se vea afectado.

H.10 Redes de comunicación

H.10.1 Redes institucionales

H.10.1.1 La UTI debe monitorear el comportamiento anómalo de las redes, los sistemas y aplicaciones y tomar medidas adecuadas para evaluar posibles incidentes de seguridad de la información.

H.10.1.2 Solamente en situaciones justificadas, a solicitud de la jefatura respectiva y con la autorización y coordinación de la UTI se permite conectar a la red alámbrica interna institucional, un equipo que no pertenezca a la CGR. Para estos casos la UTI deberá llevar un registro del equipo y garantizar que cumpla con las políticas de seguridad establecidas institucionalmente. La UTI conectará estos equipos a una red separada del resto de la plataforma y controlada en forma independiente por el firewall Institucional.

H.10.1.3 Estas conexiones alámbricas designadas para la conexión de equipos externos, estarán destinadas únicamente para brindar acceso a internet y bajo ninguna circunstancia tendrán acceso a equipos internos de la CGR.

H.10.1.4 Los activos tecnológicos conectados a la red institucional, permanentemente o en forma temporal, deberán contar como medidas de protección al menos con un programa antivirus y un firewall debidamente instalados.

H.10.1.5 La UTI establecerá zonas de seguridad diferenciadas para la conexión de los servidores institucionales, con el objetivo de segmentar la red y aplicar controles de acceso específicos según la criticidad de los sistemas y la información que albergan. Cada zona tendrá distintos perfiles de seguridad que dependen de los servicios y accesos puestos a disposición por parte de la CGR; garantizando la integridad y confidencialidad de la información.

H.10.1.6 Ningún equipo conectado a la red de la CGR podrá establecer una conexión simultánea a una red externa no autorizada. Se prohíbe la conexión de dispositivos a redes Wi-Fi públicas o privadas no gestionadas por la UTI, así como el uso de módems o dispositivos de conexión a Internet no autorizados.

H.10.2 Seguridad en redes inalámbricas

H.10.2.1 La UTI definirá las redes inalámbricas necesarias para dar servicio de conectividad a:

- Equipos de CGR con el sistema operativo Windows.
- Equipos propiedad de funcionarios, con el requerimiento de conexión permanente a las redes de la CGR.

- Equipos de visitantes o del personal con requerimiento de conexión temporal.

H.10.2.2 La UTI elaborará y mantendrá actualizadas guías de operación para cada categoría de conexión.

H.10.2.3 La UTI es la responsable de administrar las conexiones inalámbricas existentes a nivel institucional y podrá delegar en usuarios autorizados la opción de otorgar acceso a los visitantes que lo soliciten.

H.10.2.4 Las conexiones inalámbricas serán tratadas bajo los esquemas de seguridad y conectividad establecidos por la UTI.

H.10.2.5 La instalación y puesta en operación de cualquier equipo de acceso inalámbrico *(access point)* dentro de las instalaciones de la CGR, ya sea que se conecte a la red institucional o no, requiere la autorización expresa de la UTI.

H.10.2.6 La UTI debe renovar mensualmente las claves de acceso a las redes inalámbricas que no utilicen mecanismos de autenticación basados en certificados digitales.

H.10.3 Redes privadas virtuales (VPN)

H.10.3.1 El acceso al VPN se realizará mediante la autenticación del usuario, utilizando un nombre de usuario único y una contraseña personal y confidencial.

H.10.3.2 Se requiere la activación de la autenticación de dos factores (2FA) en todas las cuentas de usuario que accedan al VPN.

H.10.3.3 El acceso a la VPN se restringirá a usuarios que se encuentren en Costa Rica. Se implementarán mecanismos de control de acceso basados en la geolocalización para bloquear conexiones desde otros países. En casos excepcionales y justificados, la UTI podrá autorizar el acceso desde otros países, previa evaluación de la necesidad y la aplicación de medidas de seguridad adicionales.

H.10.3.4 La UTI debe mantener registros de actividad de la VPN para monitorear el uso adecuado y detectar posibles anomalías o intentos de acceso no autorizado.

H.11 Dispositivos de Internet de las cosas (IoT)

H.11.1 Toda implementación de una solución de Internet de las Cosas (IoT) debe ser evaluada y aprobada por la UTI y el CISO. La UTI verificará la viabilidad técnica de la solución, su compatibilidad con la infraestructura existente y la seguridad de la conexión a la red. El CISO evaluará los riesgos de seguridad asociados a la solución IoT y se asegurará de que cumpla con los requisitos de confidencialidad,

integridad y disponibilidad de la información

H.11.2 En los casos donde la implementación de una solución IoT no sea patrocinada por la UTI, esta unidad asignará un miembro de su equipo como contraparte técnica. Esta persona será el enlace entre la UTI y la unidad usuaria.

H.11.3 La UTI será la responsable de la administración de cualquier servidor necesario para la operación de una solución IoT, incluyendo la instalación, configuración, mantenimiento, seguridad y monitoreo.

H.11.4 La Unidad usuaria de los equipos IoT será la responsable de su gestión, incluyendo la configuración, operación, mantenimiento y seguridad. Asimismo, será responsable de la gestión de la información almacenada, procesada o transmitida por los dispositivos IoT.

H.11.5 La UTI tendrá la potestad de desconectar de la red institucional cualquier dispositivo IoT que determine esté poniendo en riesgo la seguridad de la información institucional.

H.11.6 Todos los dispositivos tipo IoT se deben conectar a redes independientes de las redes de datos institucionales y su conexión a otras redes incluyendo la internet será controlada por algún dispositivo de seguridad administrado por la UTI.

H.11.7 La solución de seguridad de la CGR deberá cubrir dentro de su ámbito de protección a las redes de dispositivos IoT.

H.11.8 Las pruebas de penetración (pentesting) que se realicen a la infraestructura tecnológica de la CGR deberán incluir la evaluación de la seguridad de los dispositivos IoT en operación.

H.11.9 No se permitirán conexiones entrantes desde Internet hacia los dispositivos IoT dentro de la red de la CGR. En casos excepcionales, donde un proveedor externo requiera acceso a un dispositivo IoT para tareas de mantenimiento o soporte, se deberá solicitar una autorización a la UTI. La UTI evaluará la solicitud, analizará los riesgos de seguridad, y podrá otorgar un acceso temporal.

H.11.10 Antes de la puesta en producción de cualquier dispositivo IoT, se deberán cambiar las contraseñas predeterminadas por contraseñas robustas que cumplan con las políticas de seguridad de la institución.

H.11.11 Se deberá deshabilitar el acceso remoto a los dispositivos IoT desde fuera de la red interna de la CGR.

H.11.12 Los dispositivos tipo IoT adquiridos, deben ser capaces de recibir actualizaciones de seguridad puestas a disposición por el fabricante. El proceso de actualización será responsabilidad de la unidad usuaria correspondiente y coordinado entre la unidad usuaria, la UTI y el proveedor.

H.11.13 La comunicación de datos desde y hacia los dispositivos IoT se debe manejar de forma tal que garantice la seguridad de la información transmitida.

H.11.14 En los dispositivos IoT, sólo los puertos de red estrictamente necesarios para su funcionamiento deberán estar abiertos. Todos los demás puertos deberán ser cerrados o deshabilitados para minimizar la superficie de ataque y reducir el riesgo de accesos no autorizados.

H.12 Internet y filtrado web

H.12.1 La UTI es la unidad responsable de la administración de los servicios de acceso a Internet de la CGR.

H.12.2 La UTI deberá implementar un sistema de filtrado de sitios web, que permita bloquear el acceso a sitios con contenido inapropiado, malicioso o que no estén relacionados con las actividades de la CGR.

H.12.3 Ante una solicitud formal de una jefatura, se emitirán informes de los sitios visitados por el personal a su cargo, así como el tiempo de navegación reportado por la herramienta de monitoreo, de acuerdo con la disponibilidad de almacenamiento de esta información.

H.12.4 El CISO, en colaboración con la UTI y las áreas relevantes de la organización, definirá la propuesta de los sitios que estarán permitidos y bloqueados a nivel de acceso a la Internet. Esta propuesta se le someterá al Despacho Contralor por medio del Gerente de la DGA, para su debida aprobación.

H.12.5 La UTI implementará los controles técnicos necesarios para cumplir con las recomendaciones de sitios permitidos y bloqueados definidas por el CISO y aprobadas por el Despacho Contralor.

H.12.6 Las solicitudes de apertura o bloqueo de sitios web se gestionarán a través del CISO. El personal que requiera acceso a un sitio web bloqueado o desee solicitar el bloqueo de un sitio web deberá enviar una solicitud formal al CISO, a través de los canales de comunicación establecidos. El CISO evaluará la solicitud, considerando la política de acceso a Internet y las necesidades del solicitante, y la aprobará o denegará con la debida justificación.

H.12.7 La UTI gestionará y optimizará el ancho de banda disponible para el acceso a Internet, priorizando el acceso a aplicaciones y servicios críticos para la operación de la institución y el uso por parte de clientes internos y externos.

H.13 Uso de criptografía

H.13.1 Se implementará el cifrado de datos como medida de seguridad para proteger la información de acceso restringido. La UTI definirá los estándares de cifrado, los algoritmos y las herramientas a utilizar, y proporcionará a los usuarios las instrucciones para el cifrado y descifrado de la información.

H.13.2 La UTI proporcionará al personal las herramientas de cifrado necesarias para proteger la información clasificada como de acceso restringido en sus estaciones de trabajo.

H.13.3 La clave de cifrado podrá estar ligada a la clave asignada como parte de la identidad digital definida o ser independiente, en cuyo caso la persona dueña de esta identidad es la responsable de administrar dicha clave.

H.13.4 Cuando el personal utilice una clave de cifrado independiente, deberá proporcionar una copia de seguridad de la clave a su jefatura inmediata, a través de un canal seguro y confidencial. Esta medida permitirá el acceso a la información cifrada en caso de ausencia del usuario, garantizando la continuidad de las operaciones y la disponibilidad de la información.

H.14 Ciclo de vida de desarrollo seguro de software

H.14.1 La UTI debe establecer e implementar un conjunto de reglas y directrices para el desarrollo seguro de software y sistemas de información. El objetivo es garantizar que la seguridad de la información se implemente dentro del ciclo de vida de desarrollo seguro de software y sistemas.

H.14.2 Durante el desarrollo o adquisición de aplicaciones, se deben identificar, especificar y aprobar los requisitos de seguridad de la información. Estos requisitos deben estar alineados con las políticas de seguridad de la CGR y deben considerar la confidencialidad, integridad y disponibilidad de la información.

H.14.3 La UTI debe aplicar principios de codificación segura al desarrollo de sistemas de información como la validación de entradas, la protección contra inyecciones de código, el control de acceso y la gestión de errores, para garantizar que el software sea resistente a las amenazas y vulnerabilidades.

H.14.4 Antes de la puesta en producción de una nueva aplicación o versión de software, se deben realizar pruebas de seguridad para verificar el cumplimiento de los

requisitos de seguridad de la información. Estas pruebas deben incluir, entre otras, pruebas de penetración, análisis de vulnerabilidades y pruebas de seguridad de las aplicaciones.

H.14.5 La UTI debe dirigir, monitorear y revisar las actividades relacionadas con el desarrollo de sistemas de información subcontratados para garantizar que se implementen las medidas de seguridad de la información requeridas.

H.14.6 Los entornos de desarrollo, pruebas y producción de aplicaciones se deben mantener separados, tanto física como lógicamente, y protegidos con los debidos controles y roles de acceso.

H.14.7 La información utilizada en los entornos de prueba debe ser cuidadosamente seleccionada, priorizando el uso de datos ficticios o anonimizados que no comprometan la integridad y confidencialidad de la información real. En caso de ser indispensable utilizar información sensible, se aplicarán técnicas de enmascaramiento de datos para ocultar o modificar los datos sensibles.

H.14.8 Las pruebas de auditoría y otras actividades de aseguramiento que impliquen la evaluación de los sistemas de información se deben planificar y coordinar entre el equipo auditor y la UTI.

H.15 Repositorio Institucional de Software

H.15.1 La plataforma de repositorio institucional se utilizará principalmente para almacenar y gestionar el código fuente, la documentación y otros activos de información relacionados con los proyectos de la CGR.

H.15.2 Para garantizar la seguridad de la información, no se permite almacenar información de acceso restringido en repositorios públicos; cualquier repositorio que contenga información sensible deberá configurarse como privado y con los permisos de acceso adecuados.

H.15.3 Todo acceso a bases de datos, servicios externos u otros recursos que requieran autenticación dentro de los proyectos de la CGR se realizará mediante el uso de variables de entorno o mecanismos de gestión de secretos dedicados. Se prohíbe explícitamente la inclusión de credenciales directamente en el código fuente, archivos de configuración almacenados en los repositorios de control de versiones, o cualquier otro medio que pueda exponerlas de forma insegura.

H.15.4 Todo el código que forme parte de un proyecto oficial o tenga un carácter institucional deberá gestionarse en repositorios cuyo control y propiedad resida en

la CGR, siguiendo los procedimientos y controles de acceso establecidos.

H.15.5 Se permite la creación y uso de repositorios personales por parte de los usuarios para el desarrollo individual y la experimentación con código, siempre y cuando estos repositorios no contengan información institucional sensible ni código fuente de proyectos de la CGR.

H.15.6 Se deben implementar procedimientos para el respaldo periódico de los repositorios y la recuperación de la información en caso de incidentes. Estos procedimientos deben garantizar la disponibilidad, integridad y confidencialidad de la información respaldada.

I. Responsabilidad del personal

I.1 El incumplimiento de los deberes dispuestos en los presentes lineamientos podría generar responsabilidad administrativa, civil, penal o cualesquiera otras consecuencias previstas en la normativa interna de la CGR.

J. Transitorio

J.1 Las unidades correspondientes deberán elaborar y presentar al CISO, en un plazo máximo de tres meses a partir de la comunicación de las presentes directrices, un plan de implementación detallado para alcanzar los requerimientos establecidos en este documento. El CISO revisará y dará seguimiento a estos planes, informando periódicamente al superior jerárquico sobre el avance.

K. Vigencia

K.1 Los presentes lineamientos rigen a partir de su comunicación.

L. Glosario

Access Point. Dispositivo de red que permite la conexión inalámbrica de diversos activos TIC.

Activo tecnológico: equipos, recursos, herramientas y programas que se utilizan para procesar, administrar, comunicar y compartir la información mediante diversos soportes tecnológicos.

Activo de información: Cualquier dato, documento o sistema electrónico que

maneja o custodia la institución en el ejercicio de sus funciones.

Acuerdo de confidencialidad. Manifestación de la voluntad de las partes encaminada a producir la obligación de guardar y no revelar a terceros información que una de las partes desea proteger.

Acuerdo de nivel de servicio. *Service Level Agreement (SLA)*. Acuerdo escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad y seguridad de dicho servicio. También conocido como por sus siglas en inglés.

Base de datos. Cualquier archivo, registro u otro conjunto estructurado de datos que sean objeto de tratamiento o procesamiento, automatizado o manual, cualquiera que sea la modalidad de su elaboración, organización o acceso.

Ciberseguridad. Protección de activos de información digital, a través del tratamiento o administración de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados.

CISO. *Chief Information Security Officer.* Oficial de Seguridad de la Información. Es la persona responsable de la gestión de la seguridad de la información a nivel institucional.

Confidencialidad de la información. Garantía de que el acceso a cierta información previamente definida por la autoridad competente es solo para las personas autorizadas.

Criptografía. Término genérico que describe todas las técnicas o procesos que permiten cifrar la información, haciéndola inteligible y que para volver a su estado inicial requiere un proceso adicional de descifrado.

Criticidad de la información. Se considera que una información es crítica si la misma es utilizada por uno o más procesos de misión crítica de la Contraloría General.

CSIRT. *Computer Security Incident Response Team.* Grupo de Respuesta ante Incidentes de Seguridad. Se trata de un grupo de expertos responsables en la aplicación de medidas preventivas y correctivas ante incidencias que se puedan presentar relacionadas con la seguridad de la información.

Disponibilidad de la información. Servicio que garantiza que los usuarios autorizados tengan acceso a la información y a otros activos de información asociados en el lugar, momento y forma en que es requerida. Un sistema seguro debe mantener la información disponible para los usuarios.

DGA. División de Gestión de Apoyo de la CGR.

DNS. *Domain Name Server.* Son servidores que se encargan de traducir la dirección de un sitio en internet como por ejemplo www.cgr.go.cr a un número único conocido como dirección IP.

Firewall. Componente de software o hardware y software destinado a brindar protección a activos TIC, bloqueando el tráfico de datos que no tenga permitido en sus reglas.

FTP. *File transfer protocol.* Es un protocolo de red para la transferencia de archivos entre equipos conectados.

IaaS. *Infrastructure as a Service.* Modelo de contratación de servicios en la nube en donde el proveedor del servicio se encarga de entregar una infraestructura. El proveedor se encarga de la administración de la infraestructura y la CGR tiene el control sobre los sistemas operativos, almacenamiento y aplicaciones desplegadas, así como el control de los componentes de red virtualizados.

Incidente de seguridad de la información. Acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; impedimento en la operación normal de las redes, sistemas o activos informáticos; o cualquier otro acto que implique una violación a la política de seguridad de la información.

Información institucional. Información que se genera como parte de las funciones encomendadas por Constitución o por ley, que procesa o genera la CGR, pudiendo ser esta de acceso público o de acceso restringido, encontrándose la misma en formato físico o electrónico.

Integridad de la Información. Mantener con exactitud la información tal cual fue generada, sin ser alterada o destruida por personas o procesos no autorizados.

Internet de las cosas (IoT). Interconexión digital a la red internet, de objetos

cotidianos con una función particular.

ISO 27001. Norma internacional emitida por la Organización Internacional de Normalización (ISO) que describe cómo gestionar la seguridad de la información en una empresa.

ISP. *Internet Service Provider.* Empresas que prestan el servicio de conectividad a la red internet. ICE, RACSA, Telecable, Claro, son algunos de los ISP de Costa Rica.

LACNIC. *Latin America & Caribbean Network Information Center.* Es una organización no gubernamental internacional encargada de la asignación y administración de los recursos de numeración de Internet (IPv4, IPv6).

Líderes funcionales. Funcionarios responsables de la gestión y supervisión de áreas funcionales específicas dentro de la CGR, con la autoridad para tomar decisiones y asignar recursos.

Logs. Grabación secuencial ya sea en un archivo o en una base de datos, de todos los acontecimientos que afectan a un proceso particular.

MAGEFI. Manual General de Fiscalización Integral. Normativa que describe y regula los procesos de la CGR.

Malware. Programas con contenido malicioso que pueden poner en riesgo la seguridad de la información institucional.

Pentesting. Son pruebas que consisten en un ataque controlado a un sistema informático con la intención de encontrar las debilidades de seguridad del mismo.

Plan de continuidad del negocio (BCP). *Business Continuity Plan*. Es un plan logístico que establece las medidas que una organización debe tomar en cuenta para recuperar y restaurar en un tiempo aceptable, sus funciones críticas parcial o totalmente interrumpidas después de un desastre.

Plan de recuperación de desastres (DRP). *Disaster Recovery Plan*. Proporciona un enfoque estructurado para recuperarse de incidentes no previstos que ponen en peligro la infraestructura de TI, compuesta por hardware, software, redes, procesos y personas. El DRP es un componente del BCP.

Pruebas de ingeniería social. Ejercicios programados y controlados a cargo de personal debidamente autorizado, cuyo objetivo es probar el nivel de madurez del personal respecto al tema de la seguridad de la información a través de la manipulación de usuarios legítimos.

Redes Sociales: Son comunidades virtuales o plataformas que permiten conectar personas con intereses en común, dicha plataforma o comunidad es un lugar donde las personas se afilian para mantenerse informadas y donde opinan libremente sobre el mismo.

Seguridad documental. Es la seguridad que se aplica a los documentos que se encuentran en formato físico (papel).

Seguridad física. Es la seguridad que se aplica al acceso a los sitios donde se encuentre información, no importando el medio en que la misma se encuentre.

Sistema de control de acceso. Conjunto de medidas tecnológicas y organizativas que regulan el acceso a espacios físicos o recursos digitales.

Sistema de Gestión de Seguridad de la Información. Diseño, implantación y mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información, minimizando a la vez los riesgos de seguridad de la información de la organización.

Telnet. Protocolo de red que permite la comunicación entre dos computadoras para el acceso y gestión remota.

TIC. Tecnologías de Información y Comunicaciones

UGC. Unidad de Gobierno Corporativo

UGPH. Unidad de Gestión del Potencial Humano

USI. Unidad de Servicios de Información

USG. Unidad de Servicios Generales

USP. Unidad de Servicios de Proveeduría

UTI. Unidad de Tecnologías de Información

Vulnerabilidad. Debilidad en la gestión de la información que permite que un atacante comprometa la integridad, disponibilidad o confidencialidad de la misma y podrían estar relacionados con la seguridad física, documental o digital.