Edificio de la ABG
Vía. Baltra - Puerto Ayora
Teléfono: 052527414 - 052527023
Isla Santa Cruz-Galápagos

RESOLUCIÓN No. 009-DE-ABG-2015

LA DIRECCIÓN EJECUTIVA DE LA AGENCIA DE REGULACION Y CONTROL DE LA BIOSEGURIDAD Y CUARENTENA PARA GALÁPAGOS - ABG

CONSIDERANDO:

Que, el artículo 227 de la Constitución de la República del Ecuador establece que la Administración Pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, transparencia y evaluación;

Que, el artículo 233 de la Constitución de la República del Ecuador establece que ninguna servidora ni servidor público estará exento de responsabilidades por los actos realizados en el ejercicio de sus funciones, o por sus omisiones, y serán responsables administrativa, civil y penalmente por el manejo y administración de fondos, bienes o recursos públicos;

Que, la Ley Orgánica del Servicio Público, publicado en el Registro Oficial Suplemento No. 294 de 6 de octubre del 2010, en el Título III DEL REGIMEN INTERNO DE ADMINISTRACION DEL TALENTO HUMANO, se establece cuáles son los deberes, derechos y prohibiciones de las/os servidoras o servidores públicos;

Que, el artículo 7 de la Ley Orgánica de la Controlaría General del Estado, publicado en el Registro Oficial Suplemento Nro. 595 de 12 de junio del 2002 , establece que la Controlaría General del Estado, expedirá, aprobará y actualizará, normas de control interno que sirvan de marco básico para que las instituciones del Estado y sus servidores establezcan y pongan en funcionamiento su propio control interno;

Que, en el Reglamento a la Ley Orgánica de Servicio Público, expedido mediante Decreto Ejecutivo No. 710, publicado en el Registro Oficial Suplemento No. 418 de 1 de abril del 2011, en el CAPITULO V DEL REGIMEN DISCIPLINARIO, Sección 1a de la Responsabilidad Administrativa, artículo 78, dispone que en el ejercicio de la potestad administrativa disciplinaria y sin perjuicio de las responsabilidades administrativas, civiles, o indicios de responsabilidad penal en las que pudiere incurrir la o el servidor público que incumpliere sus obligaciones o contraviniere las disposiciones previstas en la LOSEP, este reglamento general, normas conexas y los reglamentos internos de cada institución que regulan sus actuaciones, la o el servidor será sancionado disciplinariamente conforme a las disposiciones establecidas en el Capítulo 4 del Título III de la LOSEP y en el presente reglamento general. Las sanciones se impondrán de conformidad con la gravedad de la falta;

Que, Mediante Acuerdo No. 166 de 19 de septiembre de 2013 la Secretaria Nacional de la Administración Pública, dispone a las entidades de la Administración Publica Central, Interinstitucional y que dependen de la Función Ejecutiva el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO 27000 para la Gestión de Seguridad de la Información. Dando un plazo de dieciocho mese para implementar el Esquema Gubernamental de Seguridad de la Información (EGSI) a excepción de las disposiciones o normas marcadas como prioritarias, las que se implementaran en un plazo de seis meses;

Que, el numeral 410-04 de las NORMAS DE CONTROL INTERNO PARA LAS ENTIDADES, ORGANISMOS DEL SECTOR PUBLICO Y PERSONAS JURIDICAS DE DERECHO

Edificio de la ABG
Vía. Baltra - Puerto Ayora
Teléfono: 052527414 - 052527023
Isla Santa Cruz-Galápagos

PRIVADO QUE DISPONGAN DE RECURSOS PUBLICOS, expedida mediante ACUERDO DE LA CONTRALORIA GENERAL DEL ESTADO Nro. 39, publicado en el Registro Oficial Suplemento No. 87 del 14 de diciembre del 2009 , establece que la máxima autoridad de la entidad aprobará las políticas y procedimientos que permitan organizar apropiadamente el área de tecnología de información y asignar el talento humano calificado e infraestructura tecnológica necesaria y la Unidad de Tecnología de Información definirá, documentará y difundirá las políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de información y comunicaciones en la organización, estos se actualizarán permanentemente e incluirán las tareas, los responsables de su ejecución, los procesos de excepción, el enfoque de cumplimiento y el control de los procesos que están normando, así como, las sanciones administrativas a que hubiere lugar si no se cumplieran;

Que, el Decreto Ejecutivo Nº 1319 publicado en el Segundo Suplemento del Registro Oficial Nº 811 del 17 de octubre de 2012, se crea la Agencia de Regulación y Control de la Bioseguridad y Cuarentena para Galápagos (ABG), como una entidad técnica de derecho público, adscrita al Ministerio del Ambiente, con personería jurídica, con autonomía administrativa, financiera, técnica y operativa; con sede en Puerto Ayora, cantón Santa Cruz, Provincia de Galápagos;

Que, el Estatuto Orgánico de Gestión Organizacional por Procesos de la Agencia de Regulación y Control de la Bioseguridad y Cuarentena para Galápagos, publicado en Edición Especial N° 31 del Registro Oficial del 29 de julio de 2013, en el Capítulo II en su Art. 4 establece la Estructura Básica alineada a la misión, entre las cuales consta como Procesos Habilitantes de Apoyo, la de Gestión Tecnológicas de Información y Comunicación;

Que, mediante Acuerdo Ministerial N° 157 registrado con el No. 2756 folio 177 de 22 de Octubre del 2012, la Ab. Marcela Aguinaga Vallejo, Ministra de Ambiente, de ese entonces, nombra a la Dra. Sandra Pía Marilyn Cruz Bedón, como Directora Ejecutiva de la Agencia de Regulación y Control de la Bioseguridad y Cuarentena para Galápagos (ABG);

Que, el Comité de Seguridad de la Información de la Agencia de Regulación y Control de la Bioseguridad y Cuarentena para Galápagos, en reunión ordinaria del 26 de mayo de 2015, aprobó por unanimidad los siguiente documentos: 1. Políticas de seguridad dela Información de la ABG; 2. Normas para el uso adecuado de los recursos tecnológicos de la ABG; y, 3. Normas para el uso del correo electrónico y acceso al internet en la ABG;

Que, mediante memorando N° ABG-SPI-2015-0066, de fecha 05 de junio del 2015, el Ing. Martín Espinoza González, Subdirector de Planificación Institucional, solicitó a la Dirección Ejecutiva de la ABG, que los documentos fueron aprobados el día 26 de mayo de 2015 por el Comité de Seguridad de la Información de la ABG, sean aprobados mediante una resolución de la Dirección Ejecutiva, antes de proceder a la implementación de los mismos.

En uso de las facultades legales y reglamentarias:

RESUELVE:

Art. 1.-Aprobar la Política de Seguridad de la Información de la Agencia de Regulación y Control de la Bioseguridad y Cuarentena para Galápagos; las Normas para el uso adecuado de los recursos tecnológicos de la ABG; y; las Normas para el uso del correo electrónico y acceso al internet en la ABG, adjuntas en quince, siete y nueve fojas útiles en su orden.

Edificio de la ABG
Vía. Baltra - Puerto Ayora
Teléfono: 052527414 - 052527023
Isla Santa Cruz-Galápagos

Art.2.- Disponer a las distintas unidades y procesos el cabal cumplimiento de la presente Política de Seguridad de la Información; las Normas para el uso adecuado de los recursos Tecnológicos; y; las Normas para el uso del correo electrónico y acceso al internet.

Art.3.- Encargarse a la Unidad de Tecnológicas de Información y Comunicación en el ejercicio de sus labores de control, vigilará el fiel cumplimiento de las disposiciones de la presente resolución.

Art. 4.-El Oficial de la Seguridad de la información conjuntamente con el Responsable de Seguridad de la Unidad de Tecnológicas de Información y Comunicación, realizará el seguimiento y cumplimiento de la Política de Seguridad de la Información de la Agencia de Regulación y Control de la Bioseguridad y Cuarentena para Galápagos; las Normas para el uso adecuado de los recursos Tecnológicos de la ABG; y; las Normas para el uso del correo electrónico y acceso al internet en la ABG.

Art. 5.-Encárguese al Responsable de Comunicación Social, la publicación inmediata de la presente resolución en la página web Institucional.

Art. 6.-La presente Resolución entrará en vigencia a partir de la fecha de suscripción.

Dado y firmado en la ciudad de Puerto Ayora, cantón Santa Cruz, provincia de Galápagos, a los 12 días del mes de junio de 2015.

Comuníquese y publíquese.-

DRA. MARILYN CRUZ B.
DIRECTORA EJECUTIVA
AGENCIA DE REGULACION Y CONTROL DE LA BIOSEGURIDAD Y CUARENTENA PARA GALAPAGOS-ABG

Ministerio del Ambiente

Agencia de Regulación y Control de la Bioseguridad y Cuarentena para Galápagos

Edificio de la ABG
Av. Baltra – Puerto Ayora
Teléfono: 052527414 – 052527023
Isla Santa Cruz-Galápagos

Memorando Nro. ABG-SPI-2015-0066

Puerto Ayora, 05 de junio de 2015

PARA: Sra. Dra. Sandra Pia Marilyn Cruz Bedon
Directora Ejecutiva

ASUNTO: Documentos para la implementación del EGSI

De mi consideración:

Adjunto al presente sírvase encontrar tres documentos que son la base principal de algunas acciones encaminadas a dar cumplimiento al Acuerdo Ministerial 166 "Esquema Gubernamental de la Seguridad de la Información (EGSI)" en nuestra entidad. Los documentos referidos son:

1. Políticas de seguridad de la ABG.
2. Normas para el uso adecuado de los recursos tecnológicos de la ABG.
3. Normas para el uso del correo electrónico e internet en la ABG.

Estos documentos fueron aprobados el día 26 de mayo de 2015 por el Comité de Seguridad de la Información de la ABG.
A la fecha se ha completado la fase de revisión, por lo cual le envío a usted con la finalidad de que los mismos sean aprobados mediante una resolución de la Dirección Ejecutiva, antes de proceder a la implementación de los mismos.

Con sentimientos de distinguida consideración.

Atentamente,

Documento firmado electrónicamente

Ing. Martín Elías Espinosa González
SUBDIRECTOR DE PLANIFICACIÓN

Anexos:
- Políticas de seguridad de la ABG.pdf
- Normas para el uso adecuado de los recursos tecnológicos en la ABG.pdf
- Normas para el uso de correo e internet en la ABG.pdf

da

Av. Baltra-Puerto Ayora
Edificio de la ABG
Telf.: 05-2527414-2527023-2524416

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA AGENCIA DE REGULACIÓN Y CONTROL DE LA BIOSEGURIDAD Y CUARENTENA PARA GALÁPAGOS.

Av. Baltra-Puerto Ayora
Edificio de la ABG
Telf.: 05-2527414-2527023-2524416

Av. Baltra-Puerto Ayora
Edificio de la ABG
Telf.: 05-2527414-2527023-2524416

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Agencia de Regulación y Control de la Bioseguridad y Cuarentena para Galápagos ABG, adapta a su marco institucional como política de seguridad de la información al Esquema Gubernamental de la Seguridad de la Información EGSI, tomando como referencia el Acuerdo Ministerial 166, publicada en el Registro Oficial Suplemento 88 de 25-sep-2013: Capítulo 1, numeral 1.1, literal b, que enmarca lo siguiente:

Las entidades de la Administración Pública Central, Dependiente e Institucional que generan, utilizan, procesan, comparten y almacenan información en medio electrónico o escrito, clasificada como pública, confidencial, reservada y no reservada, deberán aplicar el Esquema Gubernamental de Seguridad de la Información para definir los procesos, procedimientos y tecnologías a fin de garantizar la confidencialidad, integridad y disponibilidad de esa información, en los medios y el tiempo que su legitimidad lo requiera.

Las políticas de seguridad de la ABG son elaboradas con el propósito de proteger la información de la institución, esta política servirá de guía para la implementación de medidas de seguridad que contribuyan a mantener la integridad, confidencialidad y disponibilidad de los datos dentro de los sistemas de aplicación, redes, instalaciones informáticas y procedimientos manuales.

Definición.

Una política de seguridad de la información es un conjunto de reglas, directrices o procedimientos que se aplican a todas las actividades relacionadas al manejo de la información de una institución u organización, teniendo como propósito proteger la información, los recursos y la reputación de la entidad.

Cumplimiento obligatorio.

El cumplimiento de la política y estándares de seguridad de la información en la ABG, es de carácter obligatorio y su aceptación debe ser considerada como una condición por parte de todos los servidores que laboran en la institución en cualquiera de sus modalidades. Cualquier excepción debe ser documentada detallando explícitamente el motivo que justifica el no cumplimiento de la política.

Para la ejecución de la excepción el Departamento Tecnológico y el Oficial de Seguridad de la Información deben emitir el informe respectivo para que posteriormente sea aprobado por la máxima autoridad.

Organización de la seguridad.

En esta política se definen los roles y responsabilidades, con respecto a la protección de la información. Esta política se aplica a todos los servidores y usuarios de la ABG.

Todos los servidores y usuarios son responsables de mantener un entorno de trabajo seguro con respecto al manejo de la información, en tanto que el área de tecnologías y el oficial de seguridad de la información, deben monitorear el cumplimiento de la política y realizar las

Av. Baltra-Puerto Ayora
Edificio de la ABG
Telf.: 05-2527414-2527023-2524416

actualizaciones que sean necesarias producto de los cambios en el entorno informático y las necesidades institucionales.

Estructura organizacional relacionada a la Seguridad de la Información.

En la administración de la seguridad de la información participan todos los servidores de acuerdo a la función que cumpla dentro de la ABG, la estructura está diseñada de la siguiente forma:

- ✓ Unidad de Tecnologías de la Información y Comunicación (TICs)
- ✓ Oficial de seguridad
- ✓ Responsable de Seguridad de la unidad de TICs
- ✓ Unidad de Comunicación Social
- ✓ Usuario
- ✓ Propietario de la información

Es importante mencionar que las responsabilidades referentes a la seguridad de información son distribuidas dentro de toda la organización y no son de entera responsabilidad de la unidad de TICs. En ese sentido existen roles adicionales que recaen en los propietarios de la información, los custodios de información, el Oficial de Seguridad, Responsable de Seguridad de la unidad de TICs, Usuarios y Propietarios de la Información; quienes a más de las responsabilidades establecidas en el acuerdo ministerial 166 EGSI, deberán dar cumplimiento a las que se detallan a continuación.

Unidad de TICs

La unidad encargada de la administración de seguridad de información tiene como responsabilidades:

- ✓ Comunicar aspectos básicos de seguridad de información a los servidores de la ABG. Esto incluye un programa de concientización para comunicar aspectos básicos de seguridad de información y de las políticas de la ABG.
- ✓ Identificar los puntos vulnerables de la ABG e implementar los controles tecnológicos para disminuir los riesgos. Esto incluye el monitoreo de vulnerabilidades y reportes periódicos a la Dirección Ejecutiva y al oficial de seguridad.
- ✓ Realizar una evaluación periódica de vulnerabilidades de los sistemas que conforman la red de datos de la ABG.
- ✓ Colaborar en el monitorear el cumplimiento de la política de seguridad de la ABG.
- ✓ Controlar e investigar incidentes de seguridad o violaciones de seguridad en coordinación con el Oficial de Seguridad
- ✓ Verificar que cada activo informático \de la ABG haya sido asignado a un "propietario" el cual debe definir los requerimientos de seguridad como políticas de protección, perfiles de acceso, respuesta ante incidentes y sea responsable final del mismo.

Av. Baltra-Puerto Ayora
Edificio de la ABG
Telf.: 05-2527414-2527023-2524416

- ✓ Desarrollar y administrar el presupuesto de seguridad de información.
- ✓ Implementar controles definidos para los sistemas de información, incluyendo investigación e implementación de actualizaciones de seguridad de los sistemas (service packs, fixes, etc.) en coordinación con el oficial de seguridad.
- ✓ Administrar soluciones informáticas que permitan el cumplimiento del esquema de la seguridad de la información.
- ✓ Entrenar a los servidores en aspectos de seguridad de información en nuevas tecnologías o sistemas implantados.
- ✓ Asistir y administrar los procedimientos de backup, recuperación y plan de continuidad de sistemas.

Oficial de seguridad

El oficial de seguridad es responsable de monitorear el cumplimiento de la política interna, en estrecha relación con la Unidad de TICS. Por lo tanto dentro del plan operativo anual se debe incluir el presupuesto necesario para Evaluaciones Periódicas, Auditorias Informáticas, Adquisición de Equipos, Aplicativos tecnológicos y otros para la ejecución e implementación del EGSI.

Coordinar con el área de seguridad informática en la identificación de amenazas y vulnerabilidades referentes a la seguridad de información de la ABG.

En conjunto con el responsable de tecnologías será responsable de la preparación de otros documentos normativos necesarios para la implantación efectiva de las normas institucionales contenidas en este documento. La elaboración de esos documentos deberá hacerse en armonía con el EGSI.

Será responsable de la divulgación a los Directores, subdirectores, y oficinas técnicas de este y otros documentos normativos relacionados. También mantendrá actualizada esta documentación en el portal http://bioseguridadgalapagos.gob.ec lo cual realizará con el apoyo del departamento de comunicación de la ABG.

El oficial de seguridad y el departamento de informática tendrán la obligatoriedad de realizar auditorías a todos los equipos informáticos por lo menos dos veces al año o cuando la institución lo considere pertinente.

Área de comunicación

La responsabilidad del área de comunicación estará en apego estricto a los intereses institucionales, por consiguiente difundirá o comunicará de forma oportuna y cuando la ocasión lo amerite la información referente a las actividades de la ABG, de acuerdo a los lineamientos establecidos en esta política y demás disposiciones legales relacionadas al EGSI.

Av. Baltra-Puerto Ayora
Edificio de la ABG
Telf.: 05-2527414-2527023-2524416

Usuario

Se consideran usuarios a todos los servidores de la institución, así como a terceros que hagan uso de la información que se genere en la ABG.

Las responsabilidades de los usuarios, que utilizan información de la ABG como parte de su trabajo diario están definidas a continuación:

- ✓ Mantener la confidencialidad de las contraseñas de aplicaciones y sistemas.
- ✓ Reportar supuestas violaciones de la seguridad de información.
- ✓ Asegurarse de ingresar información adecuada a los sistemas.
- ✓ Adecuarse a las políticas de seguridad de la ABG.
- ✓ Utilizar la información de la ABG únicamente para los propósitos autorizados.

Propietario de Información

Los propietarios de información son los directores y responsables de las áreas, los cuales, son responsables de la información que se genera y se utiliza en las operaciones de su unidad.
Las áreas deben ser conscientes de los riesgos de tal forma que sea posible tomar decisiones para disminuir los mismos.
Entre las responsabilidades de los propietarios de información tenemos las siguientes:

- ✓ Asignar los niveles iniciales de clasificación de información.
- ✓ Revisión periódica de la clasificación de la información con el propósito de verificar que cumpla con los requerimientos institucionales.
- ✓ Asegurar que los controles de seguridad aplicados sean consistentes con la clasificación realizada.
- ✓ Determinar los criterios y niveles de acceso a la información.
- ✓ Revisar periódicamente los niveles de acceso a los sistemas a su cargo.
- ✓ Determinar los requerimientos de copias de respaldo para la información que les pertenece.
- ✓ Tomar las acciones adecuadas en caso de violaciones de seguridad.
- ✓ Verificar periódicamente la integridad y coherencia de la información producto de los procesos de su área.

Acceso por parte de terceros.

La ABG debe establecer para terceros adicional a las restricciones de acceso a la información que se aplican a los servidores, otras específicas considerando la clasificación de la información.

Av. Baltra-Puerto Ayora
Edificio de la ABG
Telf.: 05-2527414-2527023-2524416

Todo acceso por parte de personal externo debe ser abalizado por el Oficial de Seguridad y autorizado por la máxima autoridad, a solicitud de un Director de área, quien asume la responsabilidad por las acciones que puedan realizar con la información entregada.

El usuario externo debe firmar un acuerdo de no divulgación, antes de obtener la información para garantizar que la información será utilizada únicamente para lo cual fue solicitado.

Los contratos relacionados al servicio de tecnologías de información deben ser aprobados por el departamento jurídico de la ABG y en caso que afecten en cierta forma a la infraestructura tecnológica de la institución deber ser aprobados por la unidad de TICs.

En los contratos de procesamiento de datos externos se debe especificar los requerimientos de seguridad y acciones a ser tomadas en caso de incumplimiento. Todos los contratos deben incluir una cláusula donde se establezca el derecho de la ABG a nombrar un representante el cual será responsable de evaluar la estructura de control interna del proveedor y otra donde se especifique la confidencialidad de la información a la que el contratista tenga acceso.

Gestión de activos.

Los inventarios de activos ayudan a garantizar la vigencia de una protección eficaz de los recursos de información. El proceso de compilación de un inventario de activos es un aspecto importante de la administración de riesgos. Una organización debe contar con la capacidad de identificar sus activos y el valor relativo e importancia de los mismos.

Sobre la base de esta información, la ABG puede asignar niveles de protección proporcionales al valor e importancia de los activos. Se debe elaborar y mantener un inventario de los activos importantes asociados a cada sistema de información.

Cada activo debe ser claramente identificado y su propietario y clasificación en cuanto a seguridad deben ser acordados y documentados, junto con la ubicación vigente del mismo (importante cuando se emprende una recuperación posterior a una pérdida o daño). Ejemplos de activos asociados a sistemas de información son los siguientes:

Recursos de información

Bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes operativos, disposiciones relativas a sistemas de emergencia para la reposición de información perdida, información archivada y otros relacionados.

Recursos de software

Software de aplicaciones, software de sistemas, herramientas de desarrollo y utilitarios, antivirus y demás aplicativos informáticos que sean requeridos por la Institución.

Av. Baltra-Puerto Ayora
Edificio de la ABG
Telf.: 05-2527414-2527023-2524416

Activos físicos

Equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, PBXs, máquinas de fax, contestadores automáticos), medios magnéticos (cintas y discos), otros equipos técnicos (suministro de electricidad, unidades de aire acondicionado), mobiliario, lugares de emplazamiento, archivos físicos y digitales que contengan información, y otros dispositivos semejantes.

Servicios

Servicios informáticos y de comunicaciones, utilitarios generales, por Ej. Calefacción, iluminación, energía eléctrica, aire acondicionado.

Clasificación del acceso de la información

Toda la información debe de ser clasificada como Restringida, Confidencial, Uso Interno o General de acuerdo a lo definido en este capítulo. La clasificación de información debe de ser documentada por el Propietario y aprobada por la dirección o área responsable en conjunto con el Oficial de Seguridad, se puede definir la clasificación de la información de la siguiente manera:

Restringida

Información con mayor grado de sensibilidad; el acceso a esta información debe de ser autorizado caso por caso.

Confidencial

Información sensible que solo debe ser divulgada a aquellas personas que la necesiten para el cumplimiento de sus funciones.

Uso Interno

Datos generados para facilitar las operaciones diarias; deben de ser manejados de una manera discreta, pero no requiere de medidas elaboradas de seguridad.

General

Información que es generada específicamente para su divulgación a la población general de usuarios.

La clasificación asignada a un tipo de información, solo puede ser cambiada por el propietario de la información en coordinación con el Oficial de Seguridad, luego de justificar formalmente el cambio en dicha clasificación mediante el formulario correspondiente. La información que existe en más de un medio (por ejemplo, documento fuente, registro electrónico, reporte o red) debe de tener la misma clasificación sin importar el formato.

Frecuentemente, la información deja de ser sensible o crítica después de un cierto período de tiempo, o cuando la información se ha hecho pública.

Av. Baltra-Puerto Ayora
Edificio de la ABG
Telf.: 05-2527414-2527023-2524416

Este aspecto debe ser tomado en cuenta por el propietario de la información, para realizar una reclasificación de la misma, puesto que la clasificación por exceso ("over- classification") puede traducirse en gastos adicionales innecesarios para la institución.
La información debe de ser examinada para determinar el impacto en la ABG si fuera divulgada o alterada por medios no autorizados.

Si un usuario interno detecta que terceros están haciendo uso inadecuado de la información de la institución, debe reportar de manera inmediata al oficial de seguridad y a su jefe inmediato sobre tal particular, a fin de tomar las acciones que sean pertinentes.

La clasificación de la información sensible será definida por los propietarios de la información en conjunto con el Oficial de Seguridad.

Aplicación de controles para la información clasificada.

Las medidas de seguridad a ser aplicadas a los activos de información clasificados, incluyen pero no se limitan a las siguientes:

Información de la ABG almacenada en formato digital

Todo contenedor de información en medio digital (CD's, discos duros etc.) debe presentar una etiqueta con la clasificación correspondiente.

La información en formato digital clasificada como de acceso "General", puede ser almacenada en cualquier sistema de la ABG. Sin embargo se deben tomar las medidas necesarias para no mezclar información "General" con información correspondiente a otra clasificación.

Todo usuario, antes de transmitir información clasificada como "Restringida" o "Confidencial", debe asegurarse que el destinatario de la información esté autorizado a recibir dicha información, por lo tanto es obligación del usuario que entrega la información tomar las medidas necesarias para su verificación.

Todo usuario que requiere acceso a información clasificada como "Restringida" o "Confidencial", debe ser autorizado por el propietario de la misma.

Las autorizaciones de acceso a este tipo de información deben ser documentadas y supervisadas por la Unidad de TICs y el oficial de seguridad de la ABG.
La clasificación asignada a un tipo de información, solo puede ser cambiada por el propietario de la información, luego de justificar formalmente el cambio en dicha clasificación.

Información en formato digital, clasificada como "Restringida", debe ser encriptada con un método aprobado por la unidad de TICs cuando es almacenada en cualquier medio (disco duro, flash memory etc.) Es recomendable el uso de técnicas de encriptación para la información clasificada como "Restringida" o "Confidencial", transmitida a través de la red de datos de la ABG.

Av. Baltra-Puerto Ayora
Edificio de la ABG
Telf.: 05-2527414-2527023-2524416

Toda transmisión de Información clasificada como "Restringida", "Confidencial" o de "Uso Interno" realizada hacia o a través de redes externas a la ABG debe realizarse utilizando un medio de transmisión seguro o utilizando técnicas de encriptación aprobadas.

Los medios de almacenamiento , que albergan información clasificada como "Restringida", deben ser ubicados en ambientes cerrados diseñados para el almacenamiento de dicho tipo de información, para lo cual debe tomarse las seguridades y protecciones físicas del caso. Las copias de respaldo de la información contenida deben estar ubicadas en otro lugar geográficamente distinto.

Información restringida o confidencial solo debe imprimirse en equipos específicamente designados para esta tarea.

Información de la ABG almacenada en formato no digital

Todo documento o contenedor de información debe ser etiquetado como "Restringida", "Confidencial", de "Uso interno" o de Acceso "General", dependiendo de la clasificación asignada.
Todo documento clasificado como "Confidencial" o "Restringido" debe contar con una carátula en la cual se muestre la clasificación de la información que contiene.

Los activos de información correspondiente a distintos niveles de clasificación, deben ser almacenados en distintos contenedores.

El ambiente donde se almacena la información clasificada como "Restringida", debe contar con adecuados controles de acceso y asegurado cuando se encuentre sin vigilancia. El acceso debe ser permitido solo al personal formalmente autorizado, y terceros que deban ingresar al ambiente deberán estar acompañados por personal autorizado.

Los usuarios que utilizan documentos con información "Confidencial" o "Restringida" deben asegurarse de almacenarlos en lugares adecuados. De ser necesario, el uso de copias de los documentos con información "Confidencial" o "Restringida" serán destruidos los mismos si luego de su utilización dejan de ser necesarios.

Análisis de riesgo.

Los Propietarios de la información y custodios son conjuntamente responsables del desarrollo de análisis de riesgos anual de los sistemas a su cargo.

Como parte del análisis se debe identificar las aplicaciones críticas para la recuperación ante desastres, para lo cual importante identificar lo siguiente:

- ✓ Áreas vulnerables
- ✓ Posibles pérdidas potenciales de la información.

Av. Baltra-Puerto Ayora
Edificio de la ABG
Telf.: 05-2527414-2527023-2524416

- ✓ Para lo cual se debe realizar la selección de controles y objetivos para mitigar los puntos antes indicados, debiendo estos incluirse en el análisis de riesgo indicando las razones para su inclusión o exclusión.

Adicionalmente, un análisis de riesgo debe de ser revisado para su actualización luego de cualquier cambio significativo en los sistemas y/o procesos internos, en concordancia con la necesidad institucional.

Seguridad de los recursos humanos

Los estándares relacionados al personal deben ser aplicados para todo los servidores de la Institución en cualquiera de sus modalidades, y terceros que tengan acceso a la información. Para lo cual estará definido en un acuerdo de confidencialidad.

Deben de establecerse controles para comunicar los cambios del personal y los requerimientos de recursos tecnológicos a los responsables de la administración de la seguridad de la información. Es crucial que estos cambios sean atendidos a tiempo.

Seguridad en la definición de puestos de trabajo y recursos

La Unidad de Talento Humano debe de notificar informática la unidad de TICs y al Oficial de Seguridad todos los movimientos de personal, sea este por renuncia, salida, etc.

Cuando se notifique cualquier movimiento de personal, el propietario de información debe de asegurarse que la información y sus contendores físicos y digitales, dispositivos, etc., sean entregados, a la ABG, para lo cual se utilizar el formulario respectivo.

Capacitación de usuarios

Es responsabilidad del Oficial de Seguridad promover constantemente la importancia de la seguridad a todos los usuarios de los sistemas de información. El programa de concientización en seguridad debe de contener continuas capacitaciones y charlas utilizando recursos pedagógicos adecuados, cronograma de capacitación que deberá ser entregado a la unidad de Talento Humano para que se incluya en el plan de capacitación institucional.

Los usuarios deben de ser capacitados trimestralmente sobre la importancia de la seguridad de la información.
La capacitación en seguridad debe de incluir, pero no estar limitada, a los siguientes aspectos:

- ✓ Requerimientos de identificador de usuario y contraseña
- ✓ Seguridad de PC, incluyendo protección de virus
- ✓ Responsabilidades de la organización de seguridad de información
- ✓ Concientización de las técnicas utilizadas por "hackers"
- ✓ Programas de cumplimiento
- ✓ Guías de acceso a Internet

Av. Baltra-Puerto Ayora
Edificio de la ABG
Telf.: 05-2527414-2527023-2524416

- ✓ Guías de uso del correo electrónico
- ✓ Procesos de monitoreo de seguridad de la información utilizados
- ✓ Persona de contacto para información adicional

Respuesta ante incidentes de seguridad.

El personal encargado de la administración de seguridad debe ser plenamente identificado por todos los servidores de la ABG. Si un empleado de la ABG detecta o sospecha la ocurrencia de un incidente de seguridad, tiene la obligación de notificarlo al personal de seguridad informática.

Si un empleado detecta una vulnerabilidad en la seguridad de la información debe notificarlo al personal encargado de la administración de la seguridad, asimismo, está prohibido para el empleado realizar pruebas de dicha vulnerabilidad o aprovechar ésta para propósito alguno.

La unidad de TICs debe documentar todos los reportes de incidentes de seguridad. Cualquier error o falla en los sistemas debe ser notificado a soporte técnico, quién determinará si el error es indicativo de una vulnerabilidad en la seguridad, para ello debe hacer uso de la mesa de ayuda.

Las acciones disciplinarias tomadas contra los servidores o proveedores por la ocurrencia de una violación de seguridad, deben ser consistentes con la magnitud de la falta, ellas deben ser coordinadas con la unidad de Talento Humano.

Registro de fallas

El personal encargado de operar los sistemas de información debe registrar todos los errores y fallas que ocurren en el procesamiento de información o en los sistemas de comunicaciones, haciendo uso de la mesa de ayuda. Estos registros deben incluir lo siguiente:

- ✓ Nombre de la persona que reporta la falla
- ✓ Hora y fecha de ocurrencia de la falla
- ✓ Descripción del error o problema
- ✓ Responsable de solucionar el problema
- ✓ Descripción de la respuesta inicial ante el problema
- ✓ Descripción de la solución al problema
- ✓ Hora y fecha en la que se solucionó el problema

Los registros de fallas deben ser atendidos acorde a los niveles de escalamiento que establezca la unidad de TICs para la mesa de ayuda indicando la finalización del caso.. Además, estos registros deben ser almacenados para una posterior verificación.

Av. Baltra-Puerto Ayora
Edificio de la ABG
Telf.: 05-2527414-2527023-2524416

Administración de incidentes de seguridad

Todo incidente de seguridad deberá ser reportado por el usuario al jefe inmediato y este a su vez al Oficial de Seguridad, luego de reportado el mismo que debe ser investigado en coordinación con el propietario de la información. Se debe identificar la severidad del incidente para la toma de medidas correctivas.

El personal encargado de la administración de la seguridad debe realizar la investigación de los incidentes de forma rápida y confidencial.

El Oficial de Seguridad debe mantener una documentación así como la evidencia de todos los incidentes de seguridad ocurridos en la ABG, para de esta manera proceder con el ordenamiento jurídico vigente, en caso de ser necesario.

Intercambios de información y correo electrónico

Los mensajes de correo electrónico deben ser considerados como información oficial formal, y como tal están sujetos a monitoreo y auditoria por parte del Oficial del Seguridad en coordinación con la unidad de TICs

Copias de respaldo

Los usuarios de información son los responsables de mantener una copia actualizada de la información generada en dispositivos externos que serán facilitados por la Institución.

Semestralmente deben efectuarse pruebas aleatorias para probar la capacidad de restaurar información en caso sea necesario. Estas pruebas deben efectuarse en un ambiente distinto al ambiente de producción.
Los usuarios deben trabajar la carpeta personal establecida para dicho fin por la unidad de TICs, la cual se respalda de manera automática en el servidor de respaldos principal de la ABG.

La unidad de TICs deberá realizar copias de respaldo semanales del servidor principal de respaldo en otra ubicación geográficamente distinta.

Seguridad de dispositivos tecnológicos.

Se debe mantener un inventario actualizado de todo el software y hardware existente en la ABG, la responsabilidad del mantenimiento del inventario es del responsable de la unidad de TICs.

Todo movimiento de dispositivos tecnológicos debe ser requerido por el servidor responsable del mismo, para lo cual la unidad de TICs dará el visto bueno para el cumplimiento de dicho requerimiento
Es de responsabilidad del usuario, efectuar un correcto uso del equipo de cómputo que le fue asignado, así como de los programas en él instalados.

Cualquier dispositivo perteneciente a la ABG debe ser únicamente utilizada para propósitos institucionales.

Av. Baltra-Puerto Ayora
Edificio de la ABG
Telf.: 05-2527414-2527023-2524416

Solo los programas adquiridos o aprobados por la ABG, serán instalados en las computadoras de la entidad.

Factores de autenticación

Los accesos a los recursos de información deben cumplir como mínimo uno de los tres factores de autenticación:

- ✓ Factor de conocimiento: algo que solo el usuario conoce. Por ejemplo: contraseña o PIN.
- ✓ Factor de posesión: algo que solo el usuario posee. Por ejemplo: smartcard o token.
- ✓ Factor biométrico: algo propio de las características biológicas del usuario. Por ejemplo: lectores de retina o identificadores de voz.

Propiedad de la información

Toda la información generada por los servidores de la Institución, dentro del alcance de su trabajo es propiedad de la ABG.

Cada documento elaborado por los servidores de la Institución o por usuarios externos contratados por la ABG, debe contener la información de derecho de autor correspondiente.

Consideraciones de auditoria de sistemas de información.

Protección de las herramientas de auditoria

Todas las herramientas, incluyendo programas, aplicaciones, documentación y papeles de trabajo, requeridos para la auditoria de sistemas deben protegerse de amenazas posibles como se indica en esta política de seguridad.

Controles de auditoria de sistemas de información

Todas las actividades de auditoria previa a su ejecución deben ser debidamente planificadas para su correcta ejecución, para lo cual se debe considerar los siguientes:

- ✓ Minimizar cualquier interrupción de las operaciones de la ABG de cumpliendo con todas las actividades y objetivos de auditoria.
- ✓ Limitar del alcance de la evaluación en un ambiente controlado, asegurando la realización de las tareas de auditoria
- ✓ Registro de todas las actividades y desarrollo de la documentación de las tareas realizadas

Eliminación de la información

La eliminación de documentos y otras formas de información deben asegurar la confidencialidad de la información. La unidad de TICs debe hacer un borrado seguro de los dispositivos, que se dejen de usar en la ABG debido a daño u obsolencia, antes de que estos sean eliminados.

Av. Baltra-Puerto Ayora
Edificio de la ABG
Telf.: 05-2527414-2527023-2524416

En el caso de los dispositivos tecnológicos dañados o averiados fuesen sido enviados a terceros para su examen y/o reparación se deberá firmar el acuerdo de confidencialidad correspondiente y devolverlos a la ABG para el trámite interno pertinente.

Organización del Comité de Seguridad de la Información.

El comité, será responsable de monitorear el fiel cumplimiento de los servidores de la Institución en concordancia a lo determinado en el EGSI.
El comité de seguridad deberá reunirse con una frecuencia cuatrimestral, con la posibilidad de convocar reuniones de emergencia en caso de existir alguna necesidad que lo amerite.

Cumplimiento de la Política de Seguridad.

Los Directores de áreas y responsables deben asegurarse que las responsabilidades de seguridad sean cumplidas y las funciones relacionadas se ejecuten apropiadamente.
Es responsabilidad del personal encargado de la administración de la seguridad verificar el cumplimiento de las políticas de seguridad. Las excepciones deben ser reportadas a la Dirección correspondiente.

Esta política será de cumplimiento obligatorio en todas las Direcciones, Subdirecciones, Procesos y Programas de la ABG en cuanto al Sistema de Gestión de Seguridad Informática se refiere.

Vigencia.

Esta política tendrá vigencia a partir de la aprobación mediante resolución por parte de la Dirección Ejecutiva de la ABG.

Av. Baltra-Puerto Ayora
Edificio de la ABG
Telfs: 05-2527414-2527023-2524416

NORMAS PARA EL USO ADECUADO DE LOS RECURSOS TECNOLÓGICOS DE LA AGENCIA DE REGULACIÓN Y CONTROL DE LA BIOSEGURIDAD Y CUARENTENA PARA GALÁPAGOS.

Av. Baltra-Puerto Ayora
Edificio de la ABG
Telfs: 05-2527414-2527023-2524416

Introducción

Durante los últimos años, las instituciones del sector público en el Ecuador han recibido el impacto de las transformaciones que ocurren constantemente en el campo de la informática. Esto representa un reto para las instituciones que hacen uso de este recurso. Sin embargo, para que la tecnología pueda armonizar con las leyes en vigencia y la visión institucional, los recursos tecnológicos han de utilizarse responsablemente, tanto desde el punto de vista ético como legal.

Este documento normativo, por un lado, complementa las reglamentaciones existentes en la ABG; mientras que por otro, establece el marco de referencia para el desarrollo de normas y procedimientos para el uso de las distintas tecnologías de la información en la ABG.

La ABG ofrecerá a los servidores el acceso a los recursos tecnológicos de informática en un ambiente de privacidad (intimidad) y seguridad mientras protege y asegura sus propiedades e intereses físicos, intelectuales y de datos.

Estos recursos incluyen datos, archivos, aplicativo informáticos, infraestructura tecnológica, instalaciones físicas, equipos, medios de almacenaje de datos, comunicaciones de redes y voz, correo electrónico, imágenes, vídeo, medios de comunicación y otros medios de tecnología de información.

La ABG reconoce que esas tecnologías contribuyen a aumentar la productividad por lo que valora su uso tanto en la ejecución de actividades, como en la investigación en temas relacionados con las actividades que desempeña cada servidor.

También, reconoce que el uso de los avances tecnológicos deberá estar en armonía con los valores éticos y conforme a las leyes ecuatorianas y reglamentación interna de la Institución.

Base legal

Esta normativa está diseñado acorde a lo que establece el Esquema Gubernamental de Seguridad de la Información EGSI, aprobado mediante Acuerdo Ministerial 166 y publicado en el Registro Oficial Suplemento 88 de 25-sep-2013, la normativa en vigencia que rige en el ecuador relacionada a las tecnologías.

Propósito

Asegurar que los usuarios utilicen los recursos tecnológicos de la institución de forma ética, legal y responsable. Para cumplir con los objetivos institucionales.

Por otra parte, esta normativa van también dirigido a cumplir con dos funciones principales: primero, establecer las reglas generales mediante las cuales la ABG cumpla con sus obligaciones legales en el área de la tecnología;

Av. Baltra-Puerto Ayora
Edificio de la ABG
Telfs: 05-2527414-2527023-2524416

y segundo, que los servidores de la ABG hagan uso de los recursos tecnológicos de forma que se preserve tanto la integridad y legalidad de los sistemas como la dignidad de sus usuarios.

Alcance

Esta normativa aplica a todos los servidores de la Agencia de Regulación y Control de la Bioseguridad y Cuarentena para Galápagos.

Definiciones

- ✓ Usuarios: Se consideran usuarios a todos los servidores de la institución, así como a terceros que hagan uso de la información que se genere en la ABG.
  - Usuarios Internos: todos los servidores que mantienen relación laboral con la ABG
  - Usuarios externos: toda persona o institución que hacen uso de los servicios de la ABG.
- ✓ Recursos tecnológicos: todos los recursos contemplados en sistemas informáticos y telecomunicaciones.

Privacidad

La ABG supervisará o podrá restringir, conforme a la ley, el contenido de sus recursos tecnológicos de informática, y se reserva el derecho de limitar o prohibir el acceso a estos recursos cuando se violen las leyes o reglamentos vigentes, los reglamentos o políticas de la institución, o sus obligaciones contractuales.

La ABG respeta la privacidad de los usuarios, pero se reserva el derecho de inspeccionar el uso de sus recursos tecnológicos cuando así lo considere para determinar que el uso de las herramientas se realizan sin violaciones de las leyes ecuatorianas o las políticas institucionales, o cuando haya una situación de emergencia o una amenaza a la integridad o seguridad . Antes de acceder a los archivos del usuario, se comunicará sobre el particular a la persona que la ABG accederá a sus archivos para los fines que se persiga.

Cuando fuentes externas autorizadas soliciten una inspección o examen de cualquier o recurso tecnológico que sea propiedad de la Institución o que esté operado por ella, la ABG tratará la Información contenida en los sistemas como confidencial, a menos que la solicitud está respaldada por una o más de las siguientes condiciones:

- Que sea aprobada por la máxima autoridad, previo un informe del oficial de seguridad que sea requerido por el estado ecuatoriano con fines de auditoria (contraloría general del estado).
- Que sea requerida por el estado ecuatoriano (orden judicial válida).

Seguridad

La ABG proporcionará seguridad razonable contra la invasión y el daño a los archivos almacenados en sus recursos tecnológicos. Sin embargo, los usuarios internos o externos no pueden responsabilizar a la institución, o a algún servidor de la misma, por acceso no autorizado o daños a los archivos por causas naturales.

Además, la ABG no aceptará ninguna responsabilidad por daños a equipos o a archivos personales causados por fallas los sistemas informáticos de la Institución.

La ABG es dueña de los recursos tecnológicos y de la información que estos generen y tiene la responsabilidad de los recursos tecnológicos y las redes de computadoras internas usadas en todo el sistema.

La ABG también tiene los derechos de programación (software), propia o adquirida, y de toda la información que se genera, reside o se desarrolla en toda su infraestructura tecnológica, a no ser que se establezca lo contrario en un contrato. Por lo tanto, la ABG tiene la responsabilidad de administrar, proteger, y supervisar esta infraestructura tecnológica.

Los usuarios internos tienen la responsabilidad de mantener la seguridad, confidencialidad, integridad y protección de los sistemas de información de la ABG, siguiendo lo que a continuación se detalla en las siguientes normas.

Normas de cumplimiento

Se prohíbe el uso de los recursos tecnológicos para propósitos políticos, personales, comerciales, etc.

Todo usuario de los recursos tecnológicos de la ABG es responsable de proteger estos recursos, y velar por la integridad y confidencialidad de la información a la cual tiene acceso y cumplir con las condiciones de uso de la licencia correspondiente, además, tiene la obligación de respetar los derechos y la privacidad de los demás.

Se prohíbe el uso de los recursos tecnológicos a terceras personas; familiares, amigos o servidores de otras instituciones, para ello se debe tener autorización expresa de la Dirección Ejecutiva y del Oficial de seguridad de la ABG.

Los recursos tecnológicos de la ABG pueden utilizarse únicamente para propósitos institucionales (éticos y legales) y no pueden usarse para propósito que sea ilegal, inmoral, deshonesto, dañino a la reputación de la ABG o ninguno de los siguientes:

- ✓ Uso para cometer delitos u ocasionar daños a terceros.
- ✓ Terrorismo.
- ✓ Hostigamiento.
- ✓ Calumnia.

- ✓ Fraude o falsa representación, falsificación o alteración de documentos electrónicos.
- ✓ Destrucción o daños al equipo, a la programación (software), o a los datos que pertenecen a la ABG o a terceros.
- ✓ Duplicado o transmisión sin autorización de la información generada.
- ✓ Uso o duplicación de cualquier aplicativo informático para el cual no se posea una licencia legítima.
- ✓ Plagio, hurto, robo y apropiación de información u otra propiedad.
- ✓ Uso, sin autorización, de las cuentas de la computadora, códigos de acceso (contraseñas), números de identificación de las redes (direcciones ip, direcciones de correo electrónico) asignados a otras personas, de los sistemas de información y otros usos no autorizados.
- ✓ Uso de los recursos tecnológicos de forma que impida las actividades de otras personas o afecte el funcionamiento de la ABG.
- ✓ Uso de los recursos para fines comerciales o lucro personal.
- ✓ Violación a los acuerdos de licencia de programación (software).
- ✓ Violación a las políticas, normas y regulaciones para el uso de las redes internas y externas.
- ✓ Violación a la privacidad (intimidad) de otras personas.
- ✓ Divulgación o envío de material obsceno, pornográfico, sexual explícito u ofensivo, o acceder intencionalmente a ese tipo de material.
- ✓ Divulgación o envío de material contrario a la misión o a los valores de la ABG.
- ✓ Distribución intencional o negligente de virus de computadora u otros medios que alteren y dañen el funcionamiento de los recursos tecnológicos.
- ✓ Cualquier otro uso mal intencionado que pueda causar congestión en las redes de telecomunicaciones o interferir con el trabajo de otros.

Cuando un aviso de inspección sea requerido por ley u orden judicial, los usuarios recibirán notificación previa a la inspección por parte del oficial de seguridad y/o del responsable de tecnologías.

Responsabilidades

Las oficinas técnicas, tomando en consideración sus necesidades particulares, prepararán procedimientos operacionales de implantación siguiendo los parámetros mínimos establecidos en este documento.

Todos los usuarios de los recursos tecnológicos serán responsables por el uso apropiado, el fiel cumplimiento, la implantación y funcionamiento ético y legal de esta política y los procedimientos operacionales que se establezcan.

Av. Baltra-Puerto Ayora
Edificio de la ABG
Telfs: 05-2527414-2527023-2524416

Por consiguiente, la Dirección Ejecutiva de la ABG, a través de sus canales de comunicación, debe hacer accesible a los servidores este documento y otros relacionados que se generen, para su implantación.

Todo usuario tiene la responsabilidad de conocer las normas institucionales aplicables a los diferentes aspectos de los recursos tecnológicos según le corresponda, las mismas que estarán disponibles en el sitio web institucional.

El departamento tecnológico tiene la responsabilidad de administrar todas las contraseñas asignadas a cada equipo informático, de las que se hará un respaldo para la Dirección Ejecutiva, estos recursos son propiedad de la ABG.

Acciones disciplinarias

El acceso a los recursos tecnológicos de la ABG es un privilegio. Todos los usuarios deben tenerlo así en cuenta al utilizar estos recursos. El abuso de este privilegio puede ser causa de la aplicación de acciones correctivas y disciplinarias establecidas por la ABG o de una demanda legal, la acción que se tome en cada caso dependerá de sus circunstancias particulares.

Las infracciones de menor importancia relacionadas con lo que aquí se ha establecido, generalmente se resolverán directamente con la persona implicada, de acuerdo con las normas, procesos y procedimientos oficiales aplicados en la ABG.

La repetición de infracciones o incumplimientos menores o una conducta impropia de un usuario puede dar lugar a la pérdida temporal o permanente del privilegio de acceso a los recursos tecnológicos, una modificación del privilegio y, en algunos casos, suspensión, despido u otras acciones disciplinarias consistentes con las leyes ecuatorianas relacionadas en vigencia y/o reglamentaciones de la ABG.

Las violaciones más serias incluyen, pero no se limitan a: actos delictivos o ilegales; uso desautorizado de los recursos tecnológicos; tentativa de hurtar y robar contraseñas, datos, o equipos; uso o tentativas de copiar programación (software) sin la autorización requerida; daños a la infraestructura tecnológica en general.

Cualquier ofensa que viole leyes internacionales, estatales o los reglamentos de la ABG resultará en la pérdida inmediata del privilegio de acceso a los recursos tecnológicos de la ABG y será referida a los servidores correspondientes de la Institución y a las autoridades públicas externas pertinentes para las acciones correctivas correspondientes.

Segmentación del documento.

Si cualquier parte o sección de estas normas, es declarada nula por parte de la Dirección Ejecutiva, tal decisión no afectará las restantes.

Av. Baltra-Puerto Ayora
Edificio de la ABG
Telfs: 05-2527414-2527023-2524416

Derogación o enmienda

Si en cualquier momento estas políticas estén en conflicto con otra normativa, este documento puede ser enmendado o derogado por la Dirección Ejecutiva de la ABG.

Vigencia

Estas normas entrarán en vigencia a partir de la aprobación mediante resolución por parte de la Dirección Ejecutiva de la ABG.

Av. Baltra-Puerto Ayora
Edificio de la ABG
Telfs: 05-2527414-2527023-2524416

NORMAS PARA EL USO DEL CORREO ELECTRONICO INSTUCIONAL Y ACCESO AL INTERNET EN LA AGENCIA DE REGULACIÓN Y CONTROL DE LA BIOSEGURIDAD Y CUARENTENA PARA GALÁPAGOS.

Av. Baltra-Puerto Ayora
Edificio de la ABG
Telfs: 05-2527414-2527023-2524416

Introducción

Durante los últimos años, las instituciones del sector público en el Ecuador han recibido el impacto de las transformaciones que ocurren constantemente en el campo de la informática. Esto representa un reto para las instituciones que hacen uso de este recurso. Sin embargo, para que la tecnología pueda armonizar con las leyes en vigencia y la visión institucional, los recursos tecnológicos han de utilizarse responsablemente, tanto desde el punto de vista ético como legal.

Este documento normativo por un lado, complementa las reglamentaciones existentes en la ABG; mientras que por otro, establece el marco de referencia para el desarrollo de normas y procedimientos encaminadas uso del correo electrónico instucional y acceso al internet de las en la ABG.

Todo servidor de la Agencia de Regulación y control de la Bioseguridad y Cuarentena para Galápagos "ABG" con acceso a la red institucional, también tendrá acceso al uso de internet y correo electrónico.

Base legal

Esta normativa está diseñado acorde a lo que establece el Esquema Gubernamental de Seguridad de la Información EGSI, aprobado mediante Acuerdo Ministerial 166 y publicado en el Registro Oficial Suplemento 88 de 25-sep-2013, la normativa en vigencia que rige en el ecuador relacionada a las tecnologías.

Propósito

Asegurar que los usuarios hagan uso de los servicios de correo e internet de la institución de forma ética, legal y responsable. Para cumplir con los objetivos institucionales.

Por otra parte, esta normativa van también dirigido a cumplir con dos funciones principales: primero, establecer las reglas generales mediante las cuales la ABG cumpla con sus obligaciones legales en el área de la tecnología; y segundo, que los servidores de la ABG hagan uso de los recursos tecnológicos de forma que se preserve tanto la integridad y legalidad de los sistemas como la dignidad de sus usuarios.

Alcance

Esta normativa aplica a todos los servidores de la Agencia de Regulación y Control de la Bioseguridad y Cuarentena para Galápagos.

Definiciones

- ✓ Usuarios: Se consideran usuarios a todos los servidores de la institución, así como a terceros que hagan uso de la información que se genere en la ABG.
  - Usuarios Internos: todos los servidores que mantienen relación laboral con la ABG.
  - Usuarios externos: toda persona o institución que hacen uso de los servicios de la ABG.

Recursos tecnológicos: todos los recursos contemplados en sistemas informáticos y telecomunicaciones

Directrices generales

Asignación y desactivación de cuentas de correo electrónico.

Las cuentas de correo asignadas a cada servidor, tendrán una capacidad máxima de almacenamiento en el buzón de correo de 20 MB.
Las cuentas serán desactivadas inmediatamente a la fecha en la cual un servidor termine su relación contractual con la institución. Es responsabilidad de la unidad de Talento Humano, notificar a la unidad de TICs los cambios o movimientos del personal de la Institución que tengan acceso al servicio de internet, correo electrónico y otros aplicativos informáticos, ya sea por traslado administrativo, despido o renuncia, entre otros, para lo cual se deberá hacer uso del formulario correspondiente

Es responsabilidad de la unidad de Talento Humano enviar el formulario correspondiente la unidad de TICs cada vez que exista un movimiento de personal.

Quienes no utilicen correctamente su cuenta de correo institucional y de otros aplicativos que pertenezcan o haga uso la ABG, pueden ser sancionados conforme a la normativa legal en vigencia.

Cuentas de correo electrónico.

Se entiende por cuenta de correo electrónico la asignación por parte del TICs de:

Una dirección electrónica con la forma usuario@abgalapagos.gob.ec

Un buzón (espacio en disco) para almacenar los mensajes.

Una palabra clave o password para acceder de manera privada a la cuenta.

La posibilidad de enviar y recibir mensajes internos y externos utilizando la dirección electrónica asignada.

Con el fin de garantizar que la identificación del usuario en la dirección de correo sea única, se seguirán las siguientes reglas para construir cada identificación: se construirá con el primer nombre y primer apellido separado de un punto.

En caso de presentarse coincidencias en la identificación de dos usuarios se resolverá de acuerdo con el orden de procesamiento: el primer usuario recibirá la identificación antes mencionada, el segundo será alterado recurriendo al segundo nombre.

Para las personas que cuenten con direcciones de correo definidas desde hace varios años, su identificador de usuario no tendrá validez y será construido uno nuevo bajo esta regla.

La cuenta de correo electrónico es personal e intransferible, por lo que se deben tener claves seguras y no se puede compartir la cuenta. Si existen grupos de trabajo que tengan asignada una cuenta deben nombrar un usuario autorizado para manejarla. Cada persona, o el usuario autorizado es responsable por la seguridad de su cuenta y de su clave.

La primera vez que el usuario reciba su cuenta de correo, deberá cambiar su clave. Es importante indicarles que por razones de seguridad, la clave debe cambiarse mínimo cada tres meses.

Los usuarios del servicio de correo de la ABG podrán recibir y enviar mensajes desde programas (clientes) de correo establecidos por la Unidad de TICs.

Aunque la Institución cuenta con un servicio de revisión de virus para los mensajes de correo entrante, los usuarios deberán verificar que los mensajes que se reciban o se envíen no incluyan virus, para lo cual su programa antivirus deberá estar activo y mantenerse actualizado. Es responsabilidad de cada usuario verificar lo anterior, en caso de duda deberá comunicarse con la unidad de TICS de la ABG

Para reportar problemas, hacer sugerencias o realizar cualquier solicitud que tenga relación con cuentas de correo o el servicio de correo electrónico en general, debe realizarse mediante el sistema de mesa de ayuda.
Es responsabilidad de cada usuario tener copias de respaldo (backup's) de los mensajes de sus carpetas de correo y de su agenda de direcciones electrónicas.

Administración del Servicio de Correo Electrónico.

La violación de la seguridad de los sistemas de Internet y/o de la red, puede acarrear responsabilidad civil y/o penal de conformidad con la legislación vigente.
En caso de que se inicie una investigación al respecto, el departamento de informática de la ABG colaborará con las autoridades correspondientes.

La unidad de TICs, con la ayuda de herramientas especializadas, procederá con el filtrado de los archivos que vengan anexados al correo electrónico, con extensiones tales como; exe, bat, wav, mp3, mpg, entre otros que pudieran considerarse peligrosos, con el fin de garantizar la seguridad de la red.

Es obligación de los usuarios reportar a la unidad de TICs cualquier tipo de irregularidad o abuso de estos servicios, para evitar que esto le vuelva a suceder o que le ocurra a otros servidores.
El usuario se asegurará de no responder a todas las personas cuando se envíen comunicados generales o para un grupo específico de personas, a excepción de que ésta sea la finalidad de la respuesta.

La ABG se reserva el derecho de monitorear a través del sistema las cuentas que presenten un comportamiento sospechoso para su seguridad, esto no incluye acceso al contenido de los correos.

El tamaño de los mensajes con archivos adjuntos no debe exceder los 6 MB. Este tamaño puede ser chequeado por medio de las propiedades de cada archivo, desde el Explorador de Windows o bien seleccione el archivo y presione ALT+ENTER para ver el tamaño. Para esto tome en cuenta lo siguiente:

Si el archivo adjunto excede de 6 MB, y se trata de información urgente e importante a los intereses institucionales se requiere enviar un correo electrónico al responsable tecnológico con el fin de que incremente el límite para tal envío; para este propósito se requiere conocer las direcciones tanto del emisor como de lo(s) receptor(es). El administrador de correo procede a aumentar este límite, el cual será temporal y será válido únicamente para el día solicitado.

Con el fin de agilizar el envío de información, no se podrán enviar mensajes masivos (que involucre a todos los usuarios de la ABG), a menos que sea un asunto oficial. El usuario será el responsable por el contenido de los mensajes a efecto que cumplan la característica de ser mensajes oficiales y de carácter laboral.

Normas de cumplimiento

El uso de la red Internet y del correo electrónico, constituye una herramienta y recursos que la Institución pone al servicio de sus servidores para que puedan realizar de una forma más eficiente y eficaz sus labores y así contribuyan al logro de los objetivos y metas institucionales. En tal sentido se debe acatar lo establecido en el Acuerdo Ministerial 166 "Esquema Gubernamental de Seguridad de la Información EGSI" capítulo 3. Numeral 3.3. Uso aceptable de los activos y adoptar las siguientes recomendaciones.

Se prohíbe expresamente a las entidades de la Administración Pública la contratación, acceso y uso de servicios de correo electrónico en la Internet (Nube), para uso institucional o de servidores públicos, con empresas privadas o públicas cuyos centros de datos, redes (salvo la Internet), equipos, software base y de gestión de correo electrónico y cualquier elemento tecnológico necesario, se encuentren fuera del territorio nacional; y adicionalmente, si las condiciones de los servicios que tales empresas prestaren no se someten a la Constitución y Leyes Ecuatorianas.

Evitar la transferencia de cualquier tipo de archivos, a través de servicios de mensajería como, MSN Messenger, etc.
Es responsabilidad de los usuarios:

- ✓ Usar su cuenta con fines laborales de acuerdo con su función en la ABG y lo establecido en el EGSI
- ✓ Usar un lenguaje apropiado en sus mensajes.
- ✓ Se aconseja al menos revisar el asunto (subject) antes de responder un mensaje y asegúrese que los mensajes que responda vayan dirigidos a usted.
- ✓ Sea cuidadoso cuando envíe su correo. Hay algunas direcciones que pueden ir a un grupo, pero que parece ser la de una persona. Cerciórese a quién le manda datos o información.

Av. Baltra-Puerto Ayora
Edificio de la ABG
Telfs: 05-2527414-2527023-2524416

- ✓ Las expectativas para comportarse por medio de e-mail, dependen de las relaciones con una persona y el contenido de la comunicación. Las normas aprendidas en un ambiente de e-mail particular, no necesariamente aplican en general a los mensajes a través del Internet. Sea cuidadoso con los vulgarismos o acrónimos locales.
- ✓ El costo (responsabilidad) de la entrega del mensaje es compartido entre el que lo manda y quien lo recibe. Esta es una razón económica fundamental por la cual el correo no solicitado no es bienvenido.
- ✓ No enviar ni contestar cadenas de correo o cualquier otro esquema de "pirámide" de mensajes.
- ✓ No usar su cuenta para fines comerciales.
- ✓ No se debe transmitir virus o programas de uso mal intencionado.
- ✓ Los usuarios no deben leer correo ajeno ni generar o enviar correos electrónicos a nombre de otra persona sin autorización o suplantándola.

Se prohíben las violaciones de los derechos de cualquier persona o institución protegidos por derechos de autor, patentes o cualquier otra forma de propiedad intelectual. Entre otras actividades, se incluye la distribución o instalación de software sin la licencia salvo expresa autorización de la Dirección Ejecutiva, y el oficial de seguridad.

No se debe introducir software malicioso en la red o en los servidores (virus, worms, ráfagas de correo electrónico no solicitado, etc).

No revele la clave o código de su cuenta, ni permita su uso a terceros para actividades ajenas a la misión de la ABG. La prohibición incluye a terceras personas.

El usuario debe evitar suscribirse a cualquier lista de correo que genere mensajes cuyo contenido no tenga que ver con las funciones de la ABG.

Se prohíbe el uso del correo electrónico con el fin de realizar algún tipo de acoso, difamación, calumnia, con intención de intimidar, insultar o cualquier otra forma de actividad hostil, sin importar el idioma, la periodicidad o tamaño del mensaje.

Se prohíbe el envío de mensajes de correo no solicitados o no deseados, incluyendo junk mail (material publicitario enviado por correo) o cualquier otro tipo de anuncio comercial a personas que nunca han solicitado ese tipo de material (e-mail spam, mensajes electrónicos masivos, no solicitados y no autorizados en el correo electrónico).

Queda prohibida la descarga de música y video a través de cualquier aplicación o ya se mediante el uso de páginas de streaming (música, videos en línea), en caso de hacerlo debe ser con autorización expresa de la Dirección Ejecutiva y con conocimiento del Oficial de seguridad y responsable tecnológico, únicamente para fines institucionales y con monitoreo constante.

No participar en juegos de entretenimiento en línea.

Verificar que todos los archivos que se copien a su computadora no contengan virus.

Av. Baltra-Puerto Ayora
Edificio de la ABG
Telfs: 05-2527414-2527023-2524416

Emplear el menor número de instancias del explorador de Web en forma simultánea; es decir, no tener innecesariamente varias ventanas abiertas a la vez.

Si no está navegando por la Web, debe cerrar todas las ventanas abiertas de su explorador.
Corre por cuenta o riesgo del usuario cualquier información que obtenga por medio del servicio de Internet.

Los mensajes que se envíen vía Internet, serán de completa responsabilidad del usuario emisor y en todo caso deberán basarse en la racionalidad y la responsabilidad individual.
En ningún momento dichos mensajes podrán emplearse en contra de los intereses institucionales, de personas individuales, así como de ninguna otra institución.

La demanda de servicios puede ocasionalmente exceder la disponibilidad, por lo que serán establecidas las prioridades para las unidad de TICs, áreas de financiero, compras públicas y talento humano; dando la más alta prioridad a las actividades que sean más esenciales en un momento determinado.

La "navegación" en Internet queda delimitada única y exclusivamente para fines propios de la ABG, los cuales están referidos a búsqueda de información necesaria para la elaboración, ampliación o referencia de temas relacionados con el trabajo de la Institución.

Se prohíbe el uso de Internet para cualquier actividad que sea lucrativa o comercial de carácter individual o privado.

No se podrá acceder a sitios con contenido sexual o pornográfico, ni bajar o ver material inapropiado, no sólo referido a juegos, música, pornografía, racismo, violencia, delincuencia etc. sino a cualquier otro material inaudito, que atente contra los principios morales, sociales y en general que no se relacionen con los objetivos de la institución.

El acceso a este servicio de la ABG es una concesión que puede ser revocada en cualquier momento y sin previo aviso, si se detecta uso indebido o acción que contradiga lo dispuesto en este documento. Cualquier violación de las normas aquí descritas puede resultar en la revocatoria temporal o permanente del acceso al servidor, sin perjuicio de las sanciones contempladas en la normativa vigente.

No se deberá usar este servicio para fines no identificados con la misión de la institución y con la optimización de su eficiencia administrativa y operativa.

El uso de Internet no debe interferir negativamente con la dedicación de los usuarios a sus actividades laborales.

No se podrán cambiar las configuraciones originales dejadas por los técnicos de la unidad de TICs de la ABG.

Se prohíbe estrictamente que un dispositivo conectado a la red institucional se comunique a Internet por medio de un módem externo a la ABG. El usuario que requiera conectarse a Internet por esta modalidad, deberá obtener un permiso especial de la máxima autoridad con el aval del Oficial de Seguridad y el Responsable de TICs, para lo cual se debe utilizar el formulario correspondiente.

Responsabilidades

Es responsabilidad de la unidad de TICs, proteger la información de la institución de los riesgos externos que se encuentran en Internet, por lo que este departamento a través de la Infraestructura instalada procederá a filtrar la navegación a los sitios de internet que visitan los servidores de la institución según el contenido de las páginas, utilizando herramientas especializadas para ello.

El Oficial de seguridad a través de la Dirección Ejecutiva tendrá la responsabilidad de solicitar al departamento tecnológico, reportes o informes de la navegación en internet de los servidores de la ABG cuando lo consideren pertinente.

Acciones disciplinarias

El desacato e incumplimiento de estas normas por parte de los servidores de la ABG será causal de la aplicación de acciones correctivas y disciplinarias establecidas por la ABG o de una demanda legal. La acción que se tome en cada caso dependerá de sus circunstancias particulares.

Las infracciones de menor importancia relacionadas con lo que aquí se ha establecido, generalmente se resolverán directamente con la persona implicada, de acuerdo con las normas, procesos y procedimientos oficiales aplicados en la ABG.

La repetición de infracciones o incumplimientos menores o una conducta impropia de un usuario puede dar lugar a la pérdida temporal o permanente del privilegio de acceso a los recursos tecnológicos, una modificación del privilegio y, en algunos casos, suspensión, despido u otras acciones disciplinarias consistentes con las leyes ecuatorianas relacionadas en vigencia y/o reglamentaciones de la ABG.

Las violaciones más serias incluyen, pero no se limitan a: actos delictivos o ilegales; uso desautorizado de los recursos tecnológicos; tentativa de hurtar y robar contraseñas, datos, o equipos; uso o tentativas de copiar programación (software) sin la autorización requerida; daños a la infraestructura tecnológica en general.

Cualquier ofensa que viole leyes internacionales, estatales o los reglamentos de la ABG resultará en la pérdida inmediata del privilegio de acceso a los recursos tecnológicos de la ABG y será referida a los servidores correspondientes de la Institución y a las autoridades públicas externas pertinentes para las acciones correctivas correspondientes.

Actualización y Segmentación del documento

Esta norma puede ser actualizada acorde a la necesidad institucional, lo cual podrá hacerlo el oficial de seguridad, con autorización expresa de la Dirección Ejecutiva de la ABG.
Si cualquier parte o sección de la norma es declarado nulo por la Dirección Ejecutiva, tal decisión no afectará las restantes.

Derogación o enmienda

Si en cualquier momento esta normativa entre en conflicto con otra normativa, este documento puede ser enmendado o derogado por la Dirección Ejecutiva de la ABG.

Vigencia

Estas normas entrarán en vigencia a partir de la aprobación mediante resolución por parte de la Dirección Ejecutiva de la ABG.