Secretaría de
Gestión de Riesgos

RESOLUCIÓN No. SGR-006-2014

DRA. MARÍA DEL PILAR CORNEJO DE GRUNAUER
SECRETARIA DE GESTIÓN DE RIESGOS

CONSIDERANDO:

Que, mediante Decreto Ejecutivo No 1046-A del 26 de abril del 2008, publicado en Registro Oficial No 345, de 26 de mayo de 2008, se reorganiza la Dirección Nacional de Defensa Civil, y se crea la Secretaría Técnica de Gestión de Riesgos, adscrita al Ministerio de Coordinación de Seguridad Interna y Externa, adquiriendo por este mandato, todas las competencias, atribuciones, funciones, representaciones y delegaciones constantes en leyes, reglamentos y demás instrumentos normativos que hasta ese momento le correspondían a la Dirección Nacional de Defensa Civil y a la Secretaría General del COSENA, en materia de Defensa Civil;

Que, mediante Decreto Ejecutivo No. 42 del 10 de septiembre del 2009, la Secretaría Técnica de Gestión de Riesgos, pasa a denominarse Secretaría Nacional de Gestión de Riesgos que ejercerá sus competencias y funciones de manera independiente, descentralizada y desconcentrada;

Que, mediante Decreto Ejecutivo No. 52 del 18 de septiembre del 2009, se nombra como Secretaria Nacional de Gestión de Riesgos a la doctora María del Pilar Cornejo Rodríguez de Grunauer;

Que, mediante Decreto Ejecutivo No. 103 del 20 de octubre del 2009, publicado en Registro Oficial No. 58, de 30 de octubre de 2009, mediante el cual se reforma el Decreto Ejecutivo No. 42, y se le da el rango de Ministro de Estado a la Secretaria Nacional de Gestión de Riesgos;

Que, mediante Decreto Ejecutivo No. 62 del 05 de agosto de 2013, suscrito por el señor Presidente Constitucional de la República del Ecuador, Econ. Rafael Correa Delgado, reforma el Estatuto del Régimen Jurídico y Administrativo de la Función Ejecutiva cambiando la denominación de la Secretaría Nacional de Gestión de Riesgos por la Secretaría de Gestión de Riesgos;

Que, mediante oficio Nº SNAP-SNADP-2013-000227-O del 25 de septiembre de 2013, dirigido a la Dra. María del Pilar Cornejo de Grunauer, Secretaria de Gestión de Riesgos, el Lcdo. Cristian Castillo Peñaherrera, Secretario Nacional de la Administración Pública, adjunta el Acuerdo No. 166 de 19 de septiembre de 2013 e informa que se dispone a las entidades de la Administración Pública Central, Institucional y que depende de la Función Ejecutiva el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO 27000 para la Gestión de Seguridad de la Información;

Que, mediante memorando Nro. SGR-DES-2013-0792-M del 25 de octubre de 2013, la Dra. María del Pilar Cornejo de Grunauer, Secretaria de Gestión de Riesgos, designa a los miembros para conformar el Comité de Seguridad de la Información (CSI) de la SGR, el

mismo que estará a cargo de la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI);

Que, mediante correo institucional el Comité de Seguridad de la Información (CSI) de la SGR, remitió a la Dra. María del Pilar Cornejo de Grunauer, Secretaria de Gestión de Riesgos, el reglamento para el acceso y uso del internet y sus aplicaciones/servicios, para su revisión y aprobación;

Que, mediante disposición en correo institucional de la máxima autoridad institucional dispuso a la Coordinación General del Asesoría Jurídica, se realicen los trámites pertinentes a fin de aprobar dicho reglamento;

Que, las Tecnologías de la Información y Comunicación son herramientas imprescindibles para el cumplimiento de la gestión institucional e inter-institucional de la Administración Pública en tal virtud, deben cumplir con estándares de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información;

Que, es responsabilidad de la Secretaría de Gestión de Riesgos la implementación del Esquema Gubernamental de Seguridad de la Información, emitido por la Secretaría Nacional de la Administración Pública;

Por los antecedentes expuestos y en ejercicio de sus facultades legales, en atribución a lo establecido en el numeral 1 del artículo 154 de la Constitución de la República del Ecuador:

RESUELVO:

Artículo 1.- ACOGER el contenido del Reglamento para creación y el uso del correo electrónico institucional, remitido por Comité de Seguridad de la Información (CSI) de la Secretaría de Gestión de Riesgos.

Artículo 2.- EMITIR el Reglamento para creación y el uso del correo electrónico institucional, que se describe a continuación:

Reglamento para creación y el uso del correo electrónico institucional

El presente documento regula el uso del servicio de correo institucional y es de cumplimiento obligatorio para todos los servidores públicos de la Secretaría de Gestión de Riesgos.

Sobre la Creación de las Cuentas de Correo

1. La Unidad Administrativa de Talento Humano (UATH) solicitará la creación de un usuario y contraseña para el uso del correo electrónico institucional al servidor que de acuerdo a sus funciones consideren deban tener este servicio; esta solicitud se deberá realizar el mismo día en que el servidor entregue la documentación inicial solicitada e ingrese a la institución.

2. La solicitud de creación del usuario para el uso del correo electrónico institucional se hará mediante correo electrónico a la cuenta de soporte a usuario (tic@snriesgos.gob.ec), adjuntando el formato de *Solicitud de Creación de Usuario para Correo Electrónico* (Anexo 1).
3. El Administrador del servicio de correo electrónico institucional creará el usuario y la contraseña de acuerdo a los requerimientos enviados a la cuenta de soporte.
4. Todas las cuentas de correo electrónico institucional tendrán el siguiente formato: el login será la letra inicial y el apellido del usuario y snriesgos.gob.ec es el dominio de correo electrónico Institucional
5. Los login de las cuentas de correo electrónico estarán conformados por la primera letra del nombre del funcionario y su primer apellido. La sintaxis de la cuenta de correo será *1raLetraNombrePrimerApellido* (Ejemplo: Si el Nombre del servidor es Gonzalo Antonio Pérez Jaramillo, su usuario sería *gperez*). En caso de existir alguna cuenta con el usuario generado se utilizará: *1raLetraNombrePrimerApellido1raLetraSegundoApellido* (Ejemplo: *gperezj*) en caso de existir nuevamente coincidencia con alguna cuenta de usuario existente se deberá crear la cuenta: *1raLetraNombre1raLetraSegundoNombrePrimerApellido1raLetraSegundoApellido* (Ejemplo: *gaperezj*).
6. La Dirección de Tecnologías de la Información y Comunicaciones (TIC) asignará un límite de espacio máximo de almacenamiento para cada cuenta de correo electrónico, acorde a las funciones y responsabilidades que el servidor desempeñe.
7. La UATH confirmará al servidor que la cuenta ha sido creada, así como indicará el usuario asignado y la contraseña temporal.

TIC configurará los parámetros requeridos en la máquina asignada para el servidor, para que este pueda usar la cuenta de correo.

Sobre el Uso del Correo Electrónico

1. El correo electrónico institucional es un servicio que debe ser usado exclusivamente para las tareas propias de las funciones que se desarrollan en la institución y no debe utilizarse para ningún otro fin.
2. El usuario y contraseña del correo electrónico institucional es personal e intransferible, es de responsabilidad del servidor salvaguardar su contraseña.

3. En todo momento se debe usar un lenguaje apropiado, evitando palabras ofensivas o altisonantes. En caso de que se reciba un correo que incumpla con lo manifestado se deberá informar a la UATH.

4. El usuario podrá habilitar las notificaciones automáticas en caso que el emisor requiera conocer cuando un mensaje ha sido recibido y/o leído por el destinatario.

5. Cada funcionario es el único responsable de todas las actividades realizadas con su cuenta de correo electrónico institucional (envío de correos con o sin archivos adjuntos, destrucción de los mensajes con origen desconocido, ejecución de los archivos adjuntos en correos); así como de la cantidad de mensajes que envíe.

6. Los servidores que posean cuentas de correo electrónico se deben comprometer en revisar periódicamente su bandeja de entrada y leer los correos que han recibido.

7. Para salvaguardar el rendimiento del servicio de correo electrónico y el tráfico en la red las cuentas de correo electrónico institucional permitirá enviar hasta 10 MB de archivos adjuntos.

8. En caso de recibir un correo electrónico tipo spam se deberá notificar al Administrador del servicio para que se proceda a dar seguimiento y bloqueo al mismo, luego se deberá borrar el mensaje; en caso de continuar llegando el mismo correo notificar al Oficial de Seguridad. Caso contrario el funcionario asumirá las consecuencias que pueda ocasionar la ejecución de los archivos adjuntos que dichos correos contengan.

9. Al estar por cumplirse el límite máximo de espacio de almacenamiento, el usuario deberá notificar a soporte de TIC para su respaldo respectivo.

10. En caso de bloqueo de la cuenta de correo electrónico, el jefe inmediato o a la persona que éste delegue deberá solicitar mediante correo electrónico a tic@snriesgos.gob.ec el reinicio de la contraseña; adjuntando el formato de *Solicitud de Desbloqueo de Cuenta de Usuario del Correo Electrónico* (Anexo 2).

11. En caso de ser necesario la creación de un correo tipo alias, se deberá enviar un correo electrónico a soporte de usuario y detallar cuáles son las cuentas de usuario que conformarían el alias (lista). TIC informará al solicitante una vez creada dicha cuenta alias.

Prohibiciones

1. No se debe usar la cuenta de correo electrónico personal institucional en sitios web relacionados a servicios, compra en línea, formularios y en ningún otro sitio web de dudosa procedencia y confianza. Si se requiere registrarse en sitios relacionados a la temática institucional, se deberá solicitar la aprobación por parte del Oficial de Seguridad.

2. Está prohibido usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros funcionarios. En caso de vacaciones el usuario de la cuenta de correo deberá configurar una respuesta automática indicando quién queda en reemplazo de sus actividades.

3. No realizar propagación correos tipo, ni propagar mensajes de forma masiva con contenidos inapropiados para nuestra Institución.

4. No imprima los correos electrónicos, salvo que sea estrictamente necesario.

5. Se prohíbe interceptar y/o revelar la información de los correos ajenos a su cuenta de correo institucional.

Cese de funciones de un servidor de la Institución

1. La UATH informará de manera anticipada al Administrador del Servicio el cese de las funciones dentro de la institución de algún servidor con el fin de respaldar y desactivar la cuenta de correo. Enviará un correo electrónico a soporte de usuario, adjuntando el formato de *Solicitud de Creación de Usuario para Correo Electrónico* (Anexo 1) con la Opción "*Deshabilitar Cuenta*"
2. TIC deberá realizar el respectivo respaldo, así como el almacenamiento del mismo; desactivará la cuenta indicada por TH.

Indicaciones Generales

1. TIC deberá implementar la ejecución de programas y proyectos que permitan monitorear el accionar de virus informáticos tanto en mensajes como en archivos adjuntos, antes de su ejecución.

2. Toda la información debe ser gestionada de forma centralizada y no en las estaciones de trabajo de los usuarios.

3. El envío y la conservación de la información de la Máxima Autoridad deberá encontrarse cifrada (criptografía) de datos.

4. Los correos electrónicos y los archivos adjuntos enviados son propiedad de la Institución; los cuales podrán previa autorización de la Máxima Autoridad o su delegado ser visualizados en cualquier momento.

5. Los clientes de correo electrónico autorizados son: Windows mail, Zymbra Desktop y Thunderbird.

6. Antes de realizar un mantenimiento al servidor de correo electrónico el área de TIC de la institución debe avisar con por lo menos una semana anticipación enviando un correo a todos los usuarios del servicio; en caso de que existan circunstancias

imprevistas que impidan avisar a los usuarios con anticipación, TIC informará los motivos de la paralización del servicio sin previo aviso.

7. El incumplimiento del presente reglamento por parte de los servidores de la institución será sancionado de acuerdo a lo establecido en el ordenamiento jurídico vigente.
8. El cambio de contraseña de la cuenta de correo electrónico deberá realizarse cada 4 meses.

Glosario

Alias: dirección de correo que agrupa a una o más cuentas de correo electrónico, no tienen buzón ni clave para acceder al mismo, si se envía un correo electrónico al alias le llegará a todos las cuentas que la conforman.

Bloqueo de la cuenta: cuando una cuenta de correo electrónico no puede enviar o recibir correos.

Deshabilitar cuenta: una cuenta de correo electrónico deshabilitada no podrá enviar ni recibir mensajes, el usuario dueño de esa cuenta de correo electrónico no podrá acceder en ningún momento a su cuenta; el buzón de la cuenta de correo desactivada debe ser traspasado a un medio de almacenamiento secundario para su posterior eliminación.

Spam: se denomina a los correos o mensajes basura, no solicitados, no deseados, de remitentes desconocidos o que no pertenecen a la institución; habitualmente de tipo publicitario, cadenas de mensajes, rumores, de propaganda comercial, social enviados en de manera masiva a diferentes cuentas de usuarios de correo electrónico, suelen perjudicar de alguna u otra maneras al receptor.

TIC: Dirección de Tecnología de la Información y Comunicaciones.

UATH: Unidad Administrativa de Talento Humano.

Secretaría de
Gestión de Riesgos

ANEXO 1

Gestión de Correo SGR

Acción: Crear Cuenta: ☐ Cerrar Cuenta: ☐

Información General							Área o Ubicación
Nombres	***Apellidos***	***Cédula***	***Cargo o función***	***Ciudad***	***Fecha***	***Motivo***	

Anexo 2: Solicitud de Desbloqueo de Cuenta de Usuario del Correo Electrónico

Secretaría de
Gestión de Riesgos

Reinicio de Contraseña de Correo SGR

Información General	
Nombres	
Apellidos	
Cédula	
Cargo o función	
Correo Institucional	
Motivo	

Artículo 2.- NOTIFICAR con el contenido de la presente Resolución a la Secretaría General de Administración Pública.

Artículo 3.- ENCARGAR a la Coordinación General Administrativa Financiera de la Institución el cumplimiento y aplicación del contenido de la presente Resolución.

Artículo 4.- PUBLICAR la presente Resolución y el Reglamento para creación y el uso del correo electrónico institucional en el portal web de la Secretaría de Gestión de Riesgos, que entrará en vigencia a partir de la presente fecha.

Dada y firmada en el Despacho de la Secretaría de Gestión de Riesgos, en el cantón Samborondón a los trece días del mes de enero del dos mil catorce.

DRA. MARÍA DEL PILAR CORNEJO DE GRUNAUER
SECRETARIA DE GESTIÓN DE RIESGOS