# Discurso 23 de noviembre de 2009

## Foro Regional de la UIT par alas Américas sobre Ciberseguridad[1]/ ITU Regional Cybersecurity Forum for the Americas[2]

## "Conectar el Mundo Responsablemente"/ "Connecting the World Responsibly"

## Santo Domingo, República Dominicana/Dominican Republic 23-25 de noviembre de 2009/ 23-25 November 2009

**Dr. José Rafael Vargas, Secretario de Estado y Presidente del Instituto Dominicano de las Telecomunicaciones (INDOTEL), República Dominicana**

SEÑOR JUAN ZAVATTIERO JEFE DE LA OFICINA DE LA UNION INTERNACIONAL DE LAS TELECOMUNICACIONES PARA LAS AMERICAS;

SEÑOR SOUHEIL MARINE JEFE DE LA OFICINA DE CIBER-SEGURIDAD Y APLICACIONES TICS DE LA UIT

SEÑOR JUAN ANTONIO DELGADO MIEMBRO DEL CONSEJO DIRECTIVO DEL INDOTEL

SEÑORA JOELLE EXARHACOS DIRECTORA EJECUTIVA DEL INDOTEL

QUIERO DAR LA BIENVENIDA A TODAS LAS DELEGACIONES EXTRANJERAS QUE VISITAN NUESTRO HERMOSO Y ACOGEDOR PAÍS.

ESTOY SEGURO QUE TENDRÁN LA OPORTUNIDAD DE DISFRUTAR DE LA TRADICIONAL HOSPITALIDAD DEL PUEBLO DOMINICANO, LA BELLEZA DE SUS

---

[1] Véase Foro Regional de la UIT para las Américas sobre Ciberseguridad/ITU Regional Cybersecurity Forum for Americas en el sitio web: www.itu.int/ITU-D/cyb/events/2009/santo-domingo/.

[2] See the ITU Regional Cybersecurity Forum for Americas website at: www.itu.int/ITU-D/cyb/events/2009/santo-domingo/

PLAYAS, SU MÚSICA Y ESPERO QUE LUEGO DE ESTA VISITA VOLVEREMOS A TENERLOS DE VUELTA MUY PRONTO, NO EN PLAN DE TRABAJO, SINO PARA DISFRUTAR DE SUS VACACIONES DE FAMILIA.

LAS TECNOLOGIAS CADA DIA SIGUEN DESEMPEÑANDO ROLES DECISIVOS EN LOS PROCESOS DE DESARROLLO DE NUESTROS PAISES. SIN EMBARGO, EL RAPIDO CRECIMIENTO EN EL USO DE LAS TICS, HA ABIERTO UNA NUEVA OPORTUNIDAD A LA EXPLOTACION CRIMINAL DE LAS VUNERABILIDADES EXISTENTES, AFECTANDO LAS INFRAESTRUCTURAS CRITICAS DE LOS PAISES.

TENEMOS UN GRAN RETO POR DELANTE, Y ES LA DE DAR PASOS CONCRETOS PARA HACER FRENTE A ESTAS AMENAZAS. DEBEMOS CREAR CONFIANZA Y SEGURIDAD PARA LOS USUARIOS DE LAS TICS.

LAS VENTAJAS DEL USO LAS TECNOLOGIAS SE HAN MULTIPLICADO, PERO TAMBIEN LOS RIESGOS Y PELIGROS ASOCIADOS A SU USO.

HOY EN DÍA, LOS ATAQUES POR MEDIOS ELECTRÓNICOS SON CADA VEZ MÁS SOFISTICADOS. LOS CIBER-CRIMINALES ESTÁN CADA VEZ MÁS ORGANIZADOS Y ESTÁN AMPLIANDO SUS OPERACIONES A TODOS LOS PAÍSES DEL MUNDO, OBTENIENDO MAYORES GANANCIAS CON MENORES RIESGOS.

EL FUTURO CRECIMIENTO Y EL POTENCIAL DE LA SOCIEDAD DE LA INFORMACIÓN ESTÁN EN PELIGRO Y LAS AMENAZAS SON CADA VEZ MAYORES. EN EL CIBER-ESPACIO NO EXISTEN LAS FRONTERAS: LOS CIBER-ATAQUES PUEDEN INFLIGIR UN DAÑO INALCALCULABLE EN CUESTIÓN DE MINUTOS.

EN LA CUMBRE DE MUNDIAL DE LA SOCIEDAD DE LA INFORMACIÓN, LOS LÍDERES DE LOS GOBIERNOS RECONOCIERON LOS VERDADEROS RIESGOS

PLANTEADOS POR LA CIBER-DELINCUENCIA Y CONFIARON A LA UIT EL PAPEL DETERMINANTE EN LA COORDINACIÓN DE ESFUERZOS INTERNACIONALES EN CIBER-SEGURIDAD.

POR ESO, EN RESPUESTA A ESTA SITUACIÓN, SE HA DESARROLLADO UN CRECIENTE ÉNFASIS EN LA CIBER-SEGURIDAD POR PARTE DE TODOS LOS PAÍSES, CONVIRTIÉNDOSE ASÍ EN UNO DE LOS DESAFÍOS MÁS PROFUNDOS DE NUESTRO TIEMPO.

LA PRINCIPAL PROBLEMÁTICA PARA ENFRENTAR LOS ASUNTOS DE CIBER-SEGURIDAD ES QUE NO HAY UNA ÚNICA SOLUCIÓN PARA LUCHAR CONTRA ESTAS AMENAZAS. NO ES POSIBLE LIMITAR SU SOLUCIÓN EXCLUSIVAMENTE A FACTORES LEGALES O TECNOLÓGICOS. ES NECESARIO VALORAR FACTORES PSICOLÓGICOS Y SOCIOLÓGICOS, QUE NOS PERMITAN DETERMINAR CUALES SERÁN LAS NUEVAS AMENAZAS QUE ENFRENTAREMOS EN UN FUTURO CERCANO.

LA CIBER-SEGURIDAD ES UN ASUNTO COMPLEJO, QUE REQUIERE DE REFLEXIONES PROFUNDAS, CON UNA VARIEDAD DE PERSPECTIVAS. POR ESO, RESULTA IMPERATIVO QUE PARA COMBATIR ESTAS AMENAZAS, DEBAMOS CONCURRIR EN UNA COMBINACIÓN DE VARIOS ELEMENTOS, COMO LAS MEDIDAS LEGALES, TÉCNICAS Y PROCESALES; LAS ESTRUCTURAS DE ORGANIZACIÓN; EL DESARROLLO DE CAPACIDADES Y LA COOPERACIÓN INTERNACIONAL.

EN CUANTO A LAS MEDIDAS LEGALES, DEBEMOS SEÑALAR QUE UNA LEGISLACIÓN NACIONAL SOBRE LA MATERIA, CONJUNTAMENTE CON UNA COORDINACIÓN LEGAL NACIONAL E INTERNACIONAL Y SU ADECUADA APLICACIÓN, SON ELEMENTOS IMPORTANTÍSIMOS EN LA PREVENCIÓN, DETECCIÓN Y RESPUESTA A LA CIBER-DELINCUENCIA Y AL USO INDEBIDO DE LAS TIC.

PARA ESTO SE REQUIERE DE LA ACTUALIZACIÓN DEL DERECHO PENAL SUSTANTIVO, DE PROCEDIMIENTOS Y DE POLÍTICAS PARA TRATAR LOS INCIDENTES DE CIBER-SEGURIDAD Y DE ESA FORMA PODER RESPONDER DE MANERA MAS EFECTIVA. EN MUCHOS PAÍSES DE LA REGIÓN HAN HECHO ENMIENDAS EN SUS CÓDIGOS PENALES, O ESTÁN EN CURSO LA ADOPCIÓN DE ENMIENDAS, DE ACUERDO CON CONVENCIONES Y RECOMENDACIONES INTERNACIONALES.

EN ESE SENTIDO ME PERMITO SEÑALAR QUE EN EL CASO DE LA REPÚBLICA DOMINICANA, DICHA ACTUALIZACIÓN LEGISLATIVA SE LLEVÓ A CABO MEDIANTE EL PAPEL PROTAGÓNICO Y DE MARCADO LIDERAZGO DEL INDOTEL, NO SÓLO EN LA ELABORACIÓN DE LA LEY 53-07 CONTRA CRÍMENES Y DELITOS DE ALTA TECNOLOGÍA, SINO TAMBIÉN, EN SU PROCESO DE APROBACIÓN Y HOY EN DÍA EN SU POSTERIOR EJECUCIÓN. ADEMÁS DE QUE A PARTIR DE LA APROBACIÓN DE DICHA LEGISLACIÓN, LA REPÚBLICA DOMINICANA FUE INVITADA A ADHERIRSE AL CONVENIO SOBRE CIBERCRIMINALIDAD DEL CONSEJO DE EUROPA, Y ACTUALMENTE NOS ENCONTRAMOS EN EL PROCESO DE RATIFICACIÓN DE DICHO TRATADO INTERNACIONAL POR PARTE DEL CONGRESO NACIONAL.

UN PUNTO QUE RESULTA IMPERATIVO SEÑALAR ES QUE LAS TICS SON MUY DINAMICAS, Y COMO CONSECUENCIA SE DESARROLLAN NUEVAS AMENAZAS Y NUEVOS DESAFÍOS. DEBIDO A ESTO, LA LEGISLACIÓN NACIONAL NECESITA SER CONSTANTEMENTE REVISADA Y PUESTA AL DÍA. TANTO LOS GOBIERNOS COMO LOS ACTORES DEL SECTOR PRIVADO NECESITAN OBSERVAR PERMANENTEMENTE LOS NUEVOS DESARROLLOS Y VER CÓMO A ESTAS SE LES ESTÁ DANDO UN USO INDEBIDO, PARA PROTEGER A LOS USUARIOS CON LA NUEVA LEGISLACIÓN, TENIENDO PRESENTE QUE SIEMPRE EXISTE UNA BRECHA DE TIEMPO ENTRE EL RECONOCIMIENTO DE UN CRIMEN Y LOS AJUSTES A LA LEGISLACIÓN.

UN ELEMENTO CLAVE EN EL MARCO DE UNA ESTRATEGIA NACIONAL PARA LA CIBER-SEGURIDAD Y ESPECIALMENTE EN LO QUE RESPECTA A LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS DE INFORMACIÓN, ES LA COLABORACIÓN ENTRE EL SECTOR PRIVADO Y EL GOBIERNO, PARA TRATAR LOS DESAFÍOS COMUNES DE LA SEGURIDAD NACIONAL. LA BASE DE DICHA ASOCIACIÓN PÚBLICA/PRIVADA DEBE SER LA CONFIANZA, LA CUAL RESULTA IMPRESCINDIBLE PARA ESTABLECER Y MANTENER LAS RELACIONES ENTRE AMBAS PARTES.

EN DICHO MARCO DE COOPERACIÓN DE MEDIDAS TÉCNICAS Y PROCESALES, CREEMOS CONVENIENTE EL DESARROLLO DE CAPACIDADES SOBRE CIBER-SEGURIDAD. UN EJEMPLO CLARO DE ESTO ES EL USO DE LAS HERRAMIENTAS DESARROLLADAS POR LA UIT.

LA ASOCIACIÓN DE COOPERACIÓN ENTRE LOS SECTORES PÚBLICO Y PRIVADO DEBE REQUERIR A TODAS LAS PARTES LA COMPRENSIÓN DE SUS RESPONSABILIDADES Y OBLIGACIONES PARA PROPORCIONAR LA ESTRUCTURA, LOS PROCESOS Y EL AMBIENTE REQUERIDO PARA UNA COLABORACIÓN EFECTIVA. ESTA ASOCIACIÓN DE COOPERACIÓN NECESITA QUE SE ENCUENTREN ALINEADOS LOS REQUERIMIENTOS, PRIORIDADES, METAS Y OBJETIVOS, TANTO DE LA INDUSTRIA COMO DEL GOBIERNO Y AL MISMO TIEMPO DEBE SER LO SUFICIENTEMENTE FLEXIBLE Y ADAPTABLE PARA PERMITIR COMBATIR LAS NUEVAS AMENAZAS DE UN ENTORNO EN CONSTANTE CAMBIO.

EN LO QUE SE REFIERE A LAS ESTRUCTURAS DE ORGANIZACIÓN, EL PUNTO PRINCIPAL A TRATAR DEBE SER EL MANEJO DE INCIDENTES. UNA ACTIVIDAD CLAVE PARA TRATAR LA CIBER-SEGURIDAD A NIVEL NACIONAL REQUIERE LA PREPARACIÓN, PARA LA DETECCIÓN DEL MANEJO Y LA RESPUESTA A LAS AMENAZAS A LA CIBER-SEGURIDAD A TRAVÉS DEL ESTABLECIMIENTO DE MECANISMOS DE OBSERVACIÓN, ADVERTENCIA Y CAPACIDAD DE RESPUESTA A LOS INCIDENTES.

EL MANEJO DE INCIDENTES DE MANERA EFICAZ REQUIERE LA CONJUGACIÓN DE VARIOS ELEMENTOS CLAVES, ENTRE LOS QUE PODEMOS MENCIONAR: FINANCIAMIENTO ADECUADO, RECURSOS HUMANOS CAPACITADOS, ENTRENAMIENTOS CONSTANTES, CAPACIDAD TECNOLÓGICA, RELACIONES GOBIERNO/SECTOR PRIVADO, Y BASE LEGAL APROPIADA.

LA CARENCIA DE CONOCIMIENTOS TÉCNICOS Y DE LA COMPRENSIÓN DE TODAS LAS DIMENSIONES DE LA CIBERSEGURIDAD, COMO SON LOS ASPECTOS TÉCNICOS, LEGALES, DE ORGANIZACIÓN Y HUMANOS, CONSTITUYEN UNA SERIA DEFICIENCIA QUE ES NECESARIO AFRONTAR, POR LO QUE LA EDUCACION Y CAPACITACION ES FUNDAMENTAL PARA ALCANZAR UNA CULTURA DE CIBER-SEGURIDAD.

EL SECTOR PRIVADO EN EL ÁREA DIFUSIÓN DE CONOCIMIENTO, DEBE FUNGIR COMO ESTIMULADOR, CATALIZADOR, PROMOTOR, CONSEJERO Y FACILITADOR, PARA LOGRAR AUMENTAR EL CONOCIMIENTO Y ASEGURAR QUE LOS USUARIOS SEAN CONSCIENTES DE LOS RIESGOS IMPLICADOS Y QUE CONOZCAN LAS HERRAMIENTAS QUE PUEDEN UTILIZAR PARA SALVAGUARDARSE CONTRA LAS AMENAZAS.

LA COOPERACIÓN REGIONAL E INTERNACIONAL ES EXTREMADAMENTE IMPORTANTE, YA QUE LOGRA INCENTIVAR LOS ESFUERZOS NACIONALES EN MATERIA DE CIBERSEGURIDAD, Y AL MISMO TIEMPO FACILITA LAS INTERACCIONES E INTERCAMBIOS DE BUENAS PRÁCTICAS. LOS DESAFÍOS PLANTEADOS POR LA CIBERDELINCUENCIA SON GLOBALES Y DE GRAN ENVERGADURA, Y SOLAMENTE SE PUEDEN TRATAR CON UNA ESTRATEGIA COHERENTE, DENTRO DE UN MARCO DE LA COOPERACIÓN INTERNACIONAL, CONSIDERANDO LOS DIVERSOS PAPELES DE TODOS LOS ACTORES INVOLUCRADOS Y DE LAS INICIATIVAS EXISTENTES.

COMO UN EJEMPLO DE ESTO, PODEMOS MENCIONAR LA AGENDA GLOBAL DE LA UIT SOBRE CIBER-SEGURIDAD (GCA), LA CUAL PROPORCIONA UNA PLATAFORMA PARA EL DIÁLOGO Y CONTIENE INICIATIVAS EXISTENTES DE RECONOCIDAS FUENTES DE EXPERIENCIA, PARA ELABORAR ESTRATEGIAS REGIONALES QUE LOGREN AUMENTAR LA CONFIANZA EN LAS REDES Y BRINDAR MAYOR SEGURIDAD A LA SOCIEDAD DE LA INFORMACIÓN.

FINALMENTE, PENSAMOS QUE SÓLO A TRAVÉS DE LA CONJUGACIÓN DE TODOS LOS ELEMENTOS LEGALES, TÉCNICOS, PROCESALES, ORGANIZACIONALES, EDUCATIVOS E INTERNACIONALES, PODREMOS CONTAR CON UNA ESTRATEGIA REGIONAL DE CIBER-SEGURIDAD, QUE HAGA FRENTE A LAS ACTUALES Y FUTURAS AMENAZAS DE LA CIBER-DELINCUENCIA Y GARANTIZAR LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS DE INFORMACIÓN, PARA DE ESTA MANERA CONTRIBUIR A REDUCIR LOS ATAQUES DE MANERA GLOBAL Y PODER CONSTRUIR UNA SOCIEDAD DE LA INFORMACIÓN Y DEL CONOCIMIENTO INCLUSIVA Y SEGURA.

ESTAMOS SEGUROS QUE DESDE HOY AQUÍ EN REPUBLICA DOMINICANA, ENCONTRAREMOS RESPUESTAS ADECUADAS A ESTAS INQUIETUDES. CON EL ESFUERZO Y EL APORTE DE TODOS, AYUDAREMOS A NAVEGAR SEGUROS EN EL CIBER-ESPACIO.

MUCHAS GRACIAS